

A10E/A28E/A28F
Configuration Guide

Orion Networks provides customers with comprehensive technical support and services. For any assistance, please contact our local office or company headquarters.

Website: <http://www.orionnetworks.com>

Tel: 512.646.4025

Email: info@orionnetworks.com

Address: 4262 Entry Ct STE K, Chantilly, VA 20151 USA

Notice

Copyright © 2013

Orion Networks

All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in Writing from **Orion Networks**.

 **ORION**
networks is the trademark of Orion Networks.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Preface

Objectives

This guide describes features supported by the A10E/A28E, and related configurations, including basic principles and configuration procedure of Ethernet, route, reliability, OAM, security, and QoS, and related configuration examples.

The appendix lists terms, acronyms, and abbreviations involved in this document.

By reading this guide, you can master principles and configurations of the A10E/A28E, and how to network with the A10E/A28E.

Versions




The following table lists the product versions related to this document.


Product name	Hardware version	Software version
A10E	A	NOS_4.14
A28E	A	NOS_4.14

Conventions

Symbol conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Warning	Indicates a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
 Caution	Indicates a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Symbol	Description
 Tip	Indicates a tip that may help you solve a problem or save time.

General conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Arial	Paragraphs in Warning, Caution, Notes, and Tip are in Arial.
Boldface	Names of files, directories, folders, and users are in boldface . For example, log in as user root .
<i>Italic</i>	Book titles are in <i>italics</i> .
Lucida Console	Terminal display is in <code>Lucida Console</code> .

Command conventions

Convention	Description
Boldface	The keywords of a command line are in boldface .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[]	Items (keywords or arguments) in square brackets [] are optional.
{ x y ... }	Alternative items are grouped in braces and separated by vertical bars. Only one is selected.
[x y ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x y ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x y ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. A minimum of none or a maximum of all can be selected.

GUI conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, windows, and dialog titles are in boldface . For example, click OK .
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose File > Create > Folder .

Keyboard operation

Format	Description
Key	Press the key. For example, press Enter and press Tab .
Key 1+Key 2	Press the keys concurrently. For example, pressing Ctrl+C means the two keys should be pressed concurrently.
Key 1, Key 2	Press the keys in turn. For example, pressing Alt, A means the two keys should be pressed in turn.

Mouse operation

Action	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

Contents

Preface	1
Objectives	1
Versions	1
Conventions	1
Symbol conventions	1
General conventions	2
Command conventions	2
GUI conventions.....	3
Keyboard operation	3
Mouse operation.....	3
Contents	4
Figures	16
Tables	18
1 Basic configurations	1
1.1 Accessing the device	1
1.1.1 Introduction	1
1.1.2 Accessing from the Console interface.....	2
1.1.3 Accessing from Telnet	3
1.1.4 Accessing from SSHv2	4
1.1.5 Checking configurations.....	6
1.2 CLI	6
1.2.1 Introduction	6
1.2.2 Command line level	7
1.2.3 Command line mode.....	7
1.2.4 Command line shortcuts.....	9
1.2.5 Command line help message	10
1.2.6 CLI message.....	12
1.2.7 Command line history message	13
1.2.8 Restoring default value of command line	14
1.3 Managing users	14
1.3.1 Checking configurations.....	15
1.4 Managing files	15
1.4.1 Managing BootROM files	15
1.4.2 Managing system files.....	17
1.4.3 Managing configuration files	18
1.4.4 Checking configurations.....	19

1.5 Configuring clock management.....	19
1.5.1 Configuring time and time zone.....	19
1.5.2 Configuring DST.....	20
1.5.3 Configuring NTP	20
1.5.4 Configuring SNTP	21
1.5.5 Checking configurations.....	22
1.6 Configuring interface management.....	22
1.6.1 Default configurations of interfaces.....	22
1.6.2 Configuring basic attributes for interfaces.....	23
1.6.3 Configuring flow control on interfaces	23
1.6.4 Configuring the Combo interface.....	24
1.6.5 Configuring interface rate statistics	24
1.6.6 Configuring interface statistics.....	25
1.6.7 Enabling/Disabling interfaces	25
1.6.8 Checking configurations.....	25
1.7 Configuring basic information.....	26
1.8 Task scheduling	27
1.9 Watchdog	27
1.10 Load and upgrade.....	28
1.10.1 Introduction	28
1.10.2 Configuring TFTP auto-upload method.....	29
1.10.3 Upgrading system software by BootROM.....	29
1.10.4 Upgrading system software by CLI.....	31
1.10.5 Checking configurations.....	32
1.10.6 Exampe for configuring TFTP auto-loading.....	32
2 Ethernet	34
2.1 MAC address table	34
2.1.1 Introduction	34
2.1.2 Preparing for configurations	36
2.1.3 Default configurations of MAC address table	36
2.1.4 Configuring static MAC address	36
2.1.5 Configuring multicast filtering mode for MAC address table	37
2.1.6 Configuring MAC address learning.....	37
2.1.7 Configuring MAC address limit	38
2.1.8 Configuring the aging time of MAC addresses.....	38
2.1.9 Checking configurations.....	38
2.1.10 Maintenance	39
2.1.11 Example for configuring the MAC address table.....	39
2.2 VLAN	40
2.2.1 Introduction	40
2.2.2 Preparing for configurations	42
2.2.3 Default configurations of VLAN.....	42
2.2.4 Configuring VLAN attributes	43
2.2.5 Configuring interface mode	43
2.2.6 Configuring VLAN on Access interface	44
2.2.7 Configuring VLAN on the Trunk interface	44
2.2.8 Checking configurations.....	45
2.3 QinQ.....	46
2.3.1 Introduction	46

2.3.2	Preparing for configurations	47
2.3.3	Default configurations of QinQ	47
2.3.4	Configuring basic QinQ	47
2.3.5	Configuring selective QinQ	47
2.3.6	Configuring the egress interface to Trunk mode	48
2.3.7	Checking configurations	48
2.3.8	Maintenance	48
2.3.9	Example for configuring basic QinQ	49
2.3.10	Example for configuring selective QinQ	51
2.4	VLAN mapping	54
2.4.1	Introduction	54
2.4.2	Preparing for configurations	55
2.4.3	Configuring 1:1 VLAN mapping	55
2.4.4	Configuring N:1 VLAN mapping	55
2.4.5	Checking configurations	56
2.4.6	Example for configuring VLAN mapping	56
2.5	Interface protection	58
2.5.1	Introduction	58
2.5.2	Preparing for configurations	59
2.5.3	Default configurations of interface protection	59
2.5.4	Configuring interface protection	59
2.5.5	Checking configurations	59
2.5.6	Example for configuring interface protection	60
2.6	Port mirroring	63
2.6.1	Introduction	63
2.6.2	Preparing for configurations	63
2.6.3	Default configurations of port mirroring	64
2.6.4	Configuring port mirroring on a local port	64
2.6.5	Checking configurations	65
2.6.6	Example for configuring port mirroring	65
2.7	Layer 2 protocol transparent transmission	66
2.7.1	Introduction	66
2.7.2	Preparing for configurations	67
2.7.3	Default configurations of Layer 2 protocol transparent transmission	67
2.7.4	Configuring transparent transmission parameters	67
2.7.5	Checking configuration	68
2.7.6	Maintenance	68
2.7.7	Configuring Layer 2 protocol transparent transmission	68
3	IP services	72
3.1	ARP	72
3.1.1	Introduction	72
3.1.2	Preparing for configurations	73
3.1.3	Default configurations of ARP	73
3.1.4	Configuring static ARP table entries	73
3.1.5	Configuring aging time of dynamic ARP entries	74
3.1.6	Configuring dynamic ARP entry learning mode	74
3.1.7	Checking configurations	74
3.1.8	Maintenance	74
3.1.9	Configuring ARP	75

3.2 Layer 3 interface	76
3.2.1 Introduction	76
3.2.2 Preparing for configurations	76
3.2.3 Configuring the Layer 3 interface.....	76
3.2.4 Checking configurations.....	77
3.2.5 Example for configuring Layer 3 interface to interconnect with host.....	77
3.3 Default gateway	79
3.3.1 Introduction	79
3.3.2 Preparing for configurations	79
3.3.3 Configuring the default gateway.....	79
3.3.4 Configuring static route.....	80
3.3.5 Checking configurations.....	80
3.4 DHCP Client	80
3.4.1 Introduction	80
3.4.2 Preparing for configurations	83
3.4.3 Default configurations of DHCP client.....	83
3.4.4 Applying the IP address through DHCP.....	83
3.4.5 (Optional) configuring DHCP client	84
3.4.6 (Optional) Renewing or releasing the IP address.....	84
3.4.7 Checking configurations.....	85
3.4.8 Configuring DHCP clients application.....	85
3.5 DHCP Relay	86
3.5.1 Introduction	86
3.5.2 Preparing for configurations	87
3.5.3 Default configurations of DHCP Relay.....	87
3.5.4 Configuring global DHCP Relay	87
3.5.5 Configuring interface DHCP Relay.....	87
3.5.6 Configuring the destination IP address for forwarding packets.....	88
3.5.7 (Optional) configuring DHCP Relay to support Option 82	88
3.5.8 Checking configurations.....	88
3.6 DHCP Snooping	89
3.6.1 Introduction	89
3.6.2 Preparing for configurations	90
3.6.3 Default configurations of DHCP Snooping	90
3.6.4 Configuring DHCP Snooping.....	90
3.6.5 Checking configurations.....	91
3.6.6 Example for configuring DHCP Snooping	91
3.7 DHCP options	93
3.7.1 Introduction	93
3.7.2 Preparing for configurations	94
3.7.3 Default configurations of DHCP Option	94
3.7.4 Configuring DHCP Option field.....	95
3.7.5 Checking configurations.....	95
4 QoS	96
4.1 Introduction	96
4.1.1 Service model.....	96
4.1.2 Priority trust	97
4.1.3 Traffic classification	97
4.1.4 Traffic policy	99

4.1.5 Priority mapping	100
4.1.6 Congestion management	100
4.1.7 Rate limiting based on interface and VLAN	101
4.2 Configuring basic QoS.....	102
4.2.1 Preparing for configurations	102
4.2.2 Default configurations of basic QoS.....	102
4.2.3 Enabling global QoS	102
4.2.4 Checking configurations.....	102
4.3 Configuring traffic classification and traffic policy.....	103
4.3.1 Preparing for configurations	103
4.3.2 Default configurations of traffic classification and traffic policy.....	103
4.3.3 Creating traffic classification	103
4.3.4 Configuring traffic classification rules.....	103
4.3.5 Creating token bucket and rate limiting rules.....	104
4.3.6 Creating traffic policy	105
4.3.7 Defining traffic policy mapping	105
4.3.8 Defining traffic policy operations.....	105
4.3.9 Applying traffic policy to interfaces	106
4.3.10 Checking configurations.....	107
4.3.11 Maintenance	107
4.4 Configuring priority mapping.....	107
4.4.1 Preparing for configurations	107
4.4.2 Default configurations of basic QoS.....	108
4.4.3 Configuring interface trust priority type	108
4.4.4 Configuring CoS to local priority	109
4.4.5 Configuring mapping from DSCP to local priority	109
4.4.6 Configuring mapping from local priority to DSCP	109
4.4.7 Configuring all-traffic modification on the interface	110
4.4.8 Configuring specific-traffic modification.....	110
4.4.9 Configuring CoS copying	110
4.4.10 Checking configurations.....	111
4.5 Configuring congestion management.....	111
4.5.1 Preparing for configurations	111
4.5.2 Default configurations of congestion management	112
4.5.3 Configuring SP queue scheduling.....	112
4.5.4 Configuring WRR or SP+WRR queue scheduling.....	112
4.5.5 Configuring queue transmission rate.....	112
4.5.6 Checking configurations.....	113
4.6 Configuring rate limiting based on interface and VLAN	113
4.6.1 Preparing for configurations	113
4.6.2 Configuring rate limiting based on interface	113
4.6.3 Configuring rate limiting based on VLAN	114
4.6.4 Configuring rate limiting based on QinQ	114
4.6.5 Checking configurations.....	114
4.6.6 Maintenance	114
4.7 Configuring examples.....	115
4.7.1 Example for configuring congestion management	115
4.7.2 Example for configuring rate limiting based on interface.....	117
5 Multicast.....	119

5.1 Overview	119
5.1.2 IGMP Snooping	121
5.1.3 MVR	122
5.1.4 MVR Proxy	122
5.1.5 IGMP filtering	123
5.2 Configuring IGMP Snooping	124
5.2.1 Preparing for configurations	124
5.2.2 Default configurations of IGMP Snooping	124
5.2.3 Enabling global IGMP Snooping	125
5.2.4 (Optional) enabling IGMP Snooping on VLANs	125
5.2.5 Configuring the multicast router interface	125
5.2.6 (Optional) configuring the aging time of IGMP Snooping	126
5.2.7 (Optional) configuring instance leaving	126
5.2.8 (Optional) configuring static multicast forwarding table	127
5.2.9 Checking configurations	127
5.3 Configuring MVR	128
5.3.1 Preparing for configurations	128
5.3.2 Default configurations of MVR	128
5.3.3 Configuring MVR basic information	128
5.3.4 Configuring MVR interface information	129
5.3.5 Checking configurations	130
5.4 Configuring MVR Proxy	130
5.4.1 Preparing for configurations	130
5.4.2 Default configurations of IGMP Proxy	131
5.4.3 Configuring IGMP Proxy	131
5.4.4 Checking configurations	132
5.5 Configuring IGMP filtering	132
5.5.1 Preparing for configurations	132
5.5.2 Default configurations of IGMP filtering	133
5.5.3 Enabling global IGMP filtering	133
5.5.4 Configuring IGMP filtering rules	133
5.5.5 Applying IGMP filtering rules	134
5.5.6 Configuring the maximum multicast group number	134
5.5.7 Checking configuration	135
5.6 Maintenance	135
5.7 Configuration examples	136
5.7.1 Example for configuring IGMP Snooping	136
5.7.2 Example for configuring MVR and MVR Proxy	137
5.7.3 Example for applying IGMP filtering and maximum multicast group number to the interface	140
5.7.4 Example for applying IGMP filtering and maximum multicast group number to the VLAN	142
6 Security	145
6.1 ACL	145
6.1.1 Introduction	145
6.1.2 Preparing for configurations	146
6.1.3 Default configurations of ACL	146
6.1.4 Configuring IP ACL	147
6.1.5 Configuring MAC ACL	147
6.1.6 Configuring MAP ACL	147
6.1.7 Applying ACL	150

6.1.8 Checking configurations	152
6.1.9 Maintenance	152
6.2 Secure MAC address.....	152
6.2.1 Introduction	152
6.2.2 Preparing for configurations	154
6.2.3 Default configurations of secure MAC address.....	154
6.2.4 Configuring basic functions of secure MAC address.....	154
6.2.5 Configuring static secure MAC address.....	155
6.2.6 Configuring dynamic secure MAC address	156
6.2.7 Configuring Sticky secure MAC address.....	156
6.2.8 Checking configurations.....	157
6.2.9 Maintenance	157
6.2.10 Example for configuring secure MAC address	157
6.3 Dynamic ARP inspection.....	159
6.3.1 Introduction	159
6.3.2 Preparing for configurations	161
6.3.3 Default configurations of dynamic ARP inspection.....	161
6.3.4 Configuring trusted interfaces of dynamic ARP inspection	161
6.3.5 Configuring static binding of dynamic ARP inspection	162
6.3.6 Configuring dynamic binding of dynamic ARP inspection	162
6.3.7 Configuring protection VLAN of dynamic ARP inspection	162
6.3.8 Configuring rate limiting on ARP packets on the interface	162
6.3.9 Configuring global ARP packet rate limiting auto-recovery time.....	163
6.3.10 Checking configurations.....	163
6.3.11 Example for configuring dynamic ARP inspection	163
6.4 RADIUS.....	166
6.4.1 Introduction	166
6.4.2 Preparing for configurations	166
6.4.3 Default configurations of RADIUS	167
6.4.4 Configuring RADIUS authentication.....	167
6.4.5 Configuring RADIUS accounting.....	168
6.4.6 Checking configurations.....	168
6.4.7 Example for configuring RADIUS.....	169
6.5 TACACS+	170
6.5.1 Introduction	170
6.5.2 Preparing for configurations	170
6.5.3 Default configurations of TACACS+	171
6.5.4 Configuring TACACS+ authentication.....	171
6.5.5 Configuring TACACS+ accounting.....	172
6.5.6 Configuring TACACS+ authorization	172
6.5.7 Checking configurations.....	173
6.5.8 Maintenance	173
6.5.9 Example for configuring TACACS+	173
6.6 Storm control.....	174
6.6.1 Preparing for configurations	175
6.6.2 Default configurations of storm control.....	175
6.6.3 Configuring storm control.....	175
6.6.4 Configuring DLF packet forwarding.....	176
6.6.5 Checking configurations.....	176
6.6.6 Example for configuring storm control	176

6.7 802.1x	177
6.7.1 Introduction	177
6.7.2 Preparing for configurations	179
6.7.3 Default configurations of 802.1x.....	180
6.7.4 Configuring basic functions of 802.1x.....	180
6.7.5 Configuring 802.1x re-authentication.....	181
6.7.6 Configuring 802.1x timers.....	181
6.7.7 Checking configurations.....	182
6.7.8 Maintenance	182
6.7.9 Example for configuring 802.1x	183
6.8 IP Source Guard	184
6.8.1 Introduction	184
6.8.2 Preparing for configurations	186
6.8.3 Default configurations of IP Source Guard.....	186
6.8.4 Configuring interface trust status of IP Source Guard	186
6.8.5 Configuring IP Source Guide binding	186
6.8.6 Checking configurations.....	188
6.8.7 Example for configuring IP Source Guard	188
6.9 PPPoE+	190
6.9.1 Introduction	190
6.9.2 Preparing for configurations	191
6.9.3 Default configurations of PPPoE+	192
6.9.4 Configuring basic functions of PPPoE+	192
6.9.5 Configuring PPPoE+ packet information	193
6.9.6 Checking configurations.....	195
6.9.7 Maintenance	195
6.9.8 Example for configuring PPPoE+	195
6.10 Loopback detection	197
6.10.1 Introduction	197
6.10.2 Preparing for configurations	198
6.10.3 Default configurations of loopback detection	198
6.10.4 Configuring loopback detection.....	199
6.10.5 Checking configurations.....	200
6.10.6 Maintenance	200
6.10.7 Example for configuring loopback detection	200
6.11 Line detection	202
6.11.1 Introduction	202
6.11.2 Preparing for configurations	202
6.11.3 Configuring line detection.....	202
6.11.4 Checking configurations.....	202
6.11.5 Example for configuring line detection	203
7 Reliability	205
7.1 Link aggregation	205
7.1.1 Introduction	205
7.1.2 Preparing for configurations	206
7.1.3 Default configurations of link aggregation.....	206
7.1.4 Configuring manual link aggregation	207
7.1.5 Configuring static LACP link aggregation.....	207
7.1.6 Checking configurations.....	209

7.1.7 Example for configuring manual link aggregation	209
7.1.8 Example for configuring static LACP link aggregation	211
7.2 Interface backup	213
7.2.1 Introduction	213
7.2.2 Preparing for configurations	215
7.2.3 Default configurations of interface backup.....	215
7.2.4 Configuring basic functions of interface backup.....	215
7.2.5 (Optional) configuring force switching on interfaces.....	216
7.2.6 Checking configurations.....	216
7.2.7 Example for configuring interface backup	217
7.3 Failover.....	219
7.3.1 Introduction	219
7.3.2 Preparing for configurations	219
7.3.3 Default configurations of failover	219
7.3.4 Configuring failover.....	220
7.3.5 Checking configurations.....	220
7.3.6 Example for configuring failover	221
7.4 STP	223
7.4.1 Introduction	223
7.4.2 Preparation for configuration	225
7.4.3 Default configurations of STP.....	225
7.4.4 Enabling STP.....	226
7.4.5 Configuring STP parameters.....	226
7.4.6 Checking configurations.....	227
7.4.7 Example for configuring STP	227
7.5 MSTP.....	230
7.5.1 Introduction	230
7.5.2 Preparation for configuration	233
7.5.3 Default configurations of MSTP	233
7.5.4 Enable MSTP	234
7.5.5 Configuring MST domain and its maximum hop count	234
7.5.6 Configuring root bridge/backup bridge	235
7.5.7 Configuring device interface and system priority	236
7.5.8 Configuring network diameter for switch network	236
7.5.9 Configuring inner path overhead for interfaces.....	237
7.5.10 Configuring external path cost for interface	237
7.5.11 Configuring maximum transmitting speed for interface.....	238
7.5.12 Configuring MSTP timer.....	238
7.5.13 Configuring edge interface.....	239
7.5.14 Configuring STP/MSTP mode switching	239
7.5.15 Configuring link type	240
7.5.16 Configuring root interface protection.....	240
7.5.17 Configuring interface loopguard.....	241
7.5.18 Executing mcheck operation.....	241
7.5.19 Checking configuration	242
7.5.20 Maintenance	242
7.5.21 Example for configuring MSTP	242
7.6 ERPS.....	248
7.6.1 Introduction	248
7.6.2 Preparing for configurations	248

7.6.3 Default configurations of ERPS	249
7.6.4 Creating ERPS ring.....	249
7.6.5 (Optional) creating ERPS sub-ring.....	251
7.6.6 Configuring ERPS fault detection	252
7.6.7 (Optional) configuring ERPS switching control	253
7.6.8 Checking configurations.....	254
7.6.9 Maintenance	254
7.7 RRPS.....	254
7.7.1 Introduction	254
7.7.2 Preparing for configurations	256
7.7.3 Default configurations of RRPS	257
7.7.4 Creating RRPS.....	257
7.7.5 Configuring basic functions of RRPS	257
7.7.6 Checking configuration	259
7.7.7 Maintenance	259
7.7.8 Example for configuring Ethernet ring.....	259
8 OAM	262
8.1 EFM.....	262
8.1.1 Introduction	262
8.1.2 Preparing for configurations	263
8.1.3 Default configurations of EFM	264
8.1.4 Configuring basic functions of EFM	264
8.1.5 Configuring active functions of EFM.....	265
8.1.6 Configuring passive functions of EFM.....	267
8.1.7 Checking configurations.....	268
8.1.8 Maintenance	269
8.1.9 Example for configuring EFM	269
8.2 CFM.....	270
8.2.1 Introduction	271
8.2.2 Preparing for configurations	272
8.2.3 Default configurations of CFM	273
8.2.4 Enabling CFM	274
8.2.5 Configuring basic CFM functions	274
8.2.6 Configuring fault detection	275
8.2.7 Configuring fault acknowledgement.....	277
8.2.8 Configuring fault location.....	278
8.2.9 Checking configurations.....	279
8.2.10 Maintenance	279
8.2.11 Example for configuring CFM.....	280
8.3 SLA	283
8.3.1 Introduction	283
8.3.2 Preparing for configurations	283
8.3.3 Default configurations of SLA.....	284
8.3.4 Creating SLA operations.....	284
8.3.5 Configuring SLA scheduling.....	285
8.3.6 Checking configuration	285
8.3.7 Example for configuring SLA	286
9 System management	288

9.1 SNMP	288
9.1.1 Introduction	288
9.1.2 Preparing for configurations	290
9.1.3 Default configurations of SNMP	290
9.1.4 Configuring basic functions of SNMP v1/v2c	291
9.1.5 Configuring basic functions of SNMP v3	292
9.1.6 Configuring other information of SNMP	294
9.1.7 Configuring Trap	294
9.1.8 Checking configurations	295
9.1.9 Example for configuring SNMP v1/v2c and Trap	296
9.1.10 Example for configuring SNMP v3 and Trap	298
9.2 KeepAlive	300
9.2.1 Introduction	300
9.2.2 Preparing for configurations	300
9.2.3 Default configurations of KeepAlive	301
9.2.4 Configuring KeepAlive	301
9.2.5 Checking configurations	301
9.2.6 Example for configuring KeepAlive	302
9.3 RMON	303
9.3.1 Introduction	303
9.3.2 Preparing for configurations	304
9.3.3 Default configurations of RMON	304
9.3.4 Configuring RMON statistics	304
9.3.5 Configuring RMON historical statistics	305
9.3.6 Configuring RMON alarm group	305
9.3.7 Configuring RMON event group	306
9.3.8 Checking configurations	306
9.3.9 Maintenance	307
9.3.10 Example for configuring RMON alarm group	307
9.4 LLDP	308
9.4.1 Introduction	308
9.4.2 Preparing for configurations	310
9.4.3 Default configurations of LLDP	310
9.4.4 Enabling global LLDP	311
9.4.5 Enabling interface LLDP	311
9.4.6 Configuring basic functions of LLDP	311
9.4.7 Configuring LLDP alarm	312
9.4.8 Checking configurations	312
9.4.9 Maintenance	313
9.4.10 Example for configuring basic functions of LLDP	313
9.5 Extended OAM	316
9.5.1 Introduction	316
9.5.2 Preparation for configuration	317
9.5.3 Default configurations of extended OAM	318
9.5.4 Establishing OAM link	318
9.5.5 Configure extended OAM protocols	318
9.5.6 Entering remote configuration mode	319
9.5.7 (Optional) showing remote extended OAM capacity	319
9.5.8 Configuring remote host name	320
9.5.9 Configuring MTU for the remote device	320

9.5.10 Configuring the IP address of the remote device	321
9.5.11 Configuring interface parameters on the remote device.....	321
9.5.12 Uploading and downloading files on the remote device	323
9.5.13 Configuring remote network management	326
9.5.14 Configuring remote VLAN	327
9.5.15 Configuring remote QinQ.....	328
9.5.16 Managing remote configuration files.....	329
9.5.17 Rebooting remote device.....	330
9.5.18 Checking configuration	330
9.5.19 Maintenance	331
9.5.20 Example for configuring extended OAM to manage the remote device	331
9.6 Optical module DDM.....	333
9.6.1 Introduction	333
9.6.2 Preparing for configurations	333
9.6.3 Default configurations of optical module DDM	333
9.6.4 Enabling optical module DDM	334
9.6.5 Enabling optical module DDM to send Trap messages.....	334
9.6.6 Checking configurations.....	334
9.7 System log	335
9.7.1 Introduction	335
9.7.2 Preparing for configurations	336
9.7.3 Default configurations of system log	336
9.7.4 Configuring basic information of system log.....	337
9.7.5 Configuring system log output.....	337
9.7.6 Checking configurations.....	338
9.7.7 Example for outputting system logs to log server.....	338
9.8 Power monitoring	339
9.8.1 Introduction	339
9.8.2 Preparing for configurations	339
9.8.3 Default configurations of power monitoring	339
9.8.4 Configuring power monitoring alarm	340
9.8.5 Checking configurations.....	340
9.9 CPU monitoring.....	340
9.9.1 Introduction	340
9.9.2 Preparing for configurations	341
9.9.3 Default configurations of CPU monitoring	341
9.9.4 Viewing CPU monitoring information	341
9.9.5 Configuring CPU monitoring alarm	341
9.9.6 Checking configurations.....	342
9.10 Ping	342
9.11 Traceroute	342
10 Appendix.....	344
10.1 Terms.....	344
10.2 Abbreviations.....	349

Figures

Figure 1-1 Accessing the A10E/A28E through PC connected with Console interface	2
Figure 1-2 Communication parameters configuration in Hyper Terminal	3
Figure 1-3 Networking with the A10E/A28E as Telnet server	3
Figure 1-4 A10E/A28E as Telnet client networking	4
Figure 1-5 Configuring auto-loading	32
Figure 2-1 MAC application networking	39
Figure 2-2 Dividing VLANs	41
Figure 2-3 Typical networking with basic QinQ	46
Figure 2-4 Basic QinQ networking application	49
Figure 2-5 Selective QinQ networking application	52
Figure 2-6 Networking with VLAN mapping based on single Tag	54
Figure 2-7 VLAN mapping application networking	57
Figure 2-8 Interface protection application networking	60
Figure 2-9 Port mirroring principle	63
Figure 2-10 Port mirroring application networking	65
Figure 2-11 Layer 2 protocol transparent transmission application networking	69
Figure 3-1 Configuring ARP networking application	75
Figure 3-2 Layer 3 interface configuration networking	78
Figure 3-3 DHCP typical application networking	81
Figure 3-4 Structure of DHCP packets	81
Figure 3-5 DHCP client networking	83
Figure 3-6 DHCP client networking	85
Figure 3-7 DHCP Relay application networking	86
Figure 3-8 DHCP Snooping networking	89
Figure 3-9 DHCP Snooping networking application	92
Figure 4-1 Traffic classification	98
Figure 4-2 Structure of IP packet head	98
Figure 4-3 Structure of IP priority and DSCP priority	98
Figure 4-4 Structure of VLAN packets	98
Figure 4-5 Structure of CoS priority packets	99
Figure 4-6 SP scheduling	101
Figure 4-7 WRR scheduling	101
Figure 4-8 Configure queue schedule networking	115
Figure 4-9 Rate limiting based on interface	117
Figure 5-1 Mapping relation between IPv4 multicast address and multicast MAC address	121
Figure 5-2 IGMP Snooping application networking	136
Figure 5-3 MVR application networking	138
Figure 5-4 Applying IGMP filtering on the interface	141
Figure 5-5 Applying IGMP filtering in the VLAN	143
Figure 6-1 Configuring secure MAC address	158
Figure 6-2 Principle of dynamic ARP inspection	160
Figure 6-3 Configuring dynamic ARP inspection	164

Figure 6-4 Configuring RADIUS	169
Figure 6-5 Configuring TACACS+	174
Figure 6-6 Configuring storm control	177
Figure 6-7 802.1x structure	178
Figure 6-8 Configuring 802.1x	183
Figure 6-9 IP Source Guard principle	185
Figure 6-10 Configuring IP Source Guard	189
Figure 6-11 Accessing the network through PPPoE authentication	191
Figure 6-12 Configuring PPPoE+	196
Figure 6-13 Loopback detection networking	198
Figure 6-14 Loopback detection application	201
Figure 6-15 Line detection application networking	203
Figure 7-1 Configuring manual link aggregation	210
Figure 7-2 Configuring static LACP link aggregation	211
Figure 7-3 Principles of interface backup	214
Figure 7-4 Application of interface backup in different VLANs	214
Figure 7-5 Configuring interface backup	217
Figure 7-6 Configuring failover	221
Figure 7-7 Network storm due to loopback	223
Figure 7-8 Loop networking with STP	224
Figure 7-9 VLAN packet forward failure due to RSTP	225
Figure 7-10 STP application networking	227
Figure 7-11 Basic concepts of the MSTI network	231
Figure 7-12 MSTI concepts	232
Figure 7-13 Networking of multiple spanning trees instances in MST domain	233
Figure 7-14 MSTP application networking	243
Figure 7-15 RRPS in normal status	255
Figure 7-16 RRPS in switching status	256
Figure 7-17 RRPS application networking	259
Figure 8-1 OAM classification	263
Figure 8-2 Configuring EFM	269
Figure 8-3 Different MD Levels	271
Figure 8-4 Network Sketch Map of MEP and MIP	272
Figure 8-5 CFM application	280
Figure 8-6 SLA application networking	286
Figure 9-1 Working mechanism of SNMP	289
Figure 9-2 SNMP v3 authentication mechanism	293
Figure 9-3 Configuring SNMP v1/v2c and Trap	296
Figure 9-4 Configuring SNMP v3 and Trap	298
Figure 9-5 Configuring KeepAlive	302
Figure 9-6 RMON	303
Figure 9-7 Configuring RMON alarm group	307
Figure 9-8 LLDPDU structure	309
Figure 9-9 Basic TLV structure	309
Figure 9-10 Configuring basic functions of LLDP	314
Figure 9-11 Extended OAM application networking	316
Figure 9-12 Configuring extended OAM to manage the remote device	331
Figure 9-13 Outputting system logs to log servers	338

Tables

Table 1-1 Function keys description for command line message display characteristics	13
Table 2-1 Interface mode and packet processing	41
Table 3-1 Fields definition of DHCP packets	81
Table 3-2 Common DHCP options	93
Table 4-1 Mapping relationship of local priority, DSCP priority, and CoS priority	100
Table 4-2 Mapping between local priority and queue	100
Table 4-3 Default CoS to local priority and color mapping relationship	108
Table 4-4 Default DSCP to local priority and color mapping relationship	108
Table 9-1 TLV type	309
Table 9-2 Log level	335

1 Basic configurations

This chapter introduces the basic configuration and configuration process about the A10E/A28E and provides the related configuration applications, including the following chapters:

- Accessing the device
- CLI
- Managing users
- Managing files
- Configuring clock management
- Configuring interface management
- Configuring basic information
- Task scheduling
- Watchdog
- Load and upgrade

1.1 Accessing the device

1.1.1 Introduction

The A10E/A28E can be configured and managed in Command Line Interface (CLI) mode or NView NNM network management mode.

The A10E/A28E CLI mode has a variety of configuration modes:

- Console mode: it must be used for the first configuration. The A10E/A28E supports the Console interface of RJ-45 type or USB type.
- Telnet mode: log in through the Console mode, open Telnet service on the Switch, configure Layer 3 interface IP address, set the user name and password, and then take remote Telnet configuration.
- SSHv2 mode: before accessing the A10E/A28E through SSHv2, you need to log in to the A10E/A28E and start the SSHv2 service through the Console interface.

When configuring the A10E/A28E in network management mode, you must first configure Layer 3 interface IP address in CLI, and then configure the A10E/A28E through NView NNM system.

 **Note**

The configuration steps in this manual are in command line mode.

1.1.2 Accessing from the Console interface

The Console interface is a command interface used for network device to connect to a PC with terminal emulation program. You can take this interface to configure and manage the local device. In this management method, the A10E/A28E can communicate directly without a network, so it is called out-of-band management. You can also perform configuration and management on the A10E/A28E through the Console interface when the network runs out of order.

In the below two conditions, you can only log in to the A10E/A28E and configure it through the Console port:

- The A10E/A28E is powered on to start for the first time.
- You cannot access the A10E/A28E through Telnet.

 **Note**

When logging in to the A10E/A28E through the Console interface, use the CBL-RS232-DB9F/RJ45-2m cable delivered with the A10E/A28E. If you need to make the Console serial port cable, see *A10E/A28E Hardware Description*.

If you want to access the A10E/A28E through PC via Console interface, connect Console interface and PC RS-232 serial port, as shown in Figure 1-1; then run the terminal emulation program such as Windows XP Hyper Terminal program in PC to configure communication parameters as shown in Figure 1-2, and then log in to the A10E/A28E.

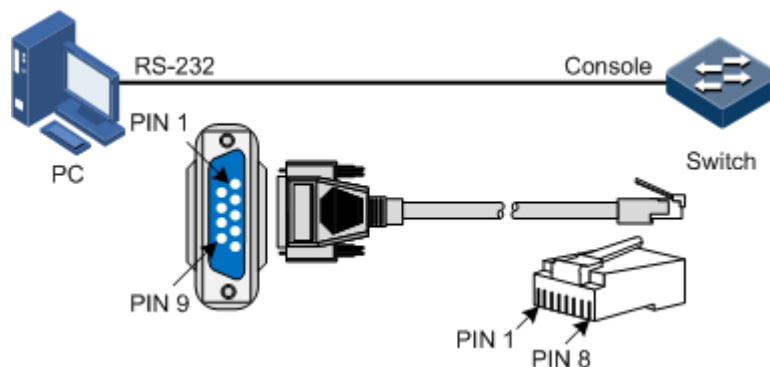


Figure 1-1 Accessing the A10E/A28E through PC connected with Console interface

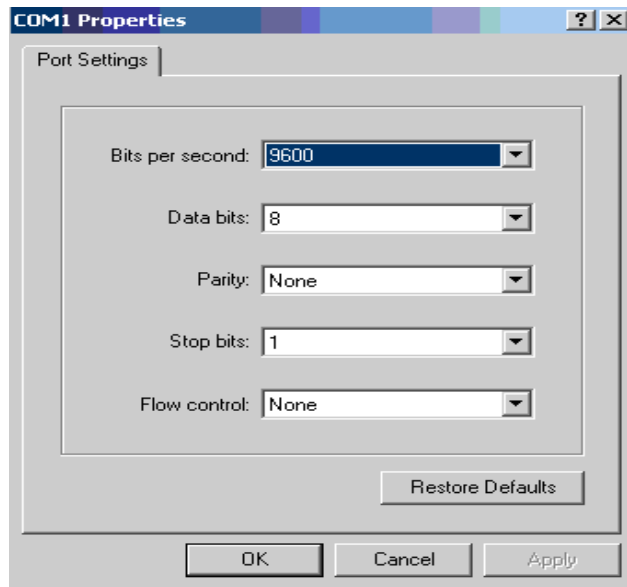


Figure 1-2 Communication parameters configuration in Hyper Terminal

 **Note**

Microsoft is not in support of Hyper Terminal since Windows Vista system. For Windows Vista or Windows 7, download Hyper Terminal program from internet. It is free to download HyperTerminal program.

1.1.3 Accessing from Telnet

You can use a PC to log in to the A10E/A28E remotely through Telnet. You can log in to an A10E/A28E from PC at first, then Telnet other A10E/A28E devices on the network. You do not need to connect a PC to each A10E/A28E.

Telnet service provided by the A10E/A28E includes:

- Telnet Server: run the Telnet client program on a PC to log in to the A10E/A28E, and take configuration and management. As shown in Figure 1-3, the A10E/A28E is providing Telnet Server service at this time.

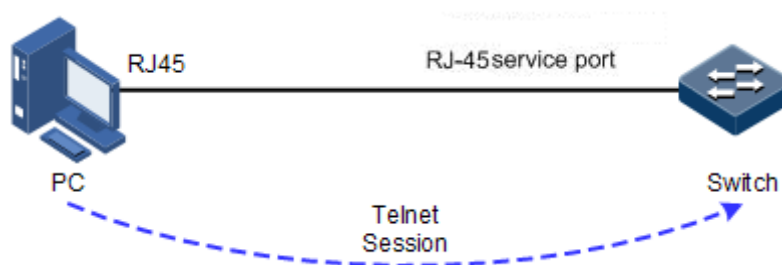


Figure 1-3 Networking with the A10E/A28E as Telnet server

Before accessing the A10E/A28E through Telnet, you need to log in to the A10E/A28E through the Console interface and start the Telnet service. Take the following configurations on the A10E/A28E that needs to start Telnet service.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface ip if-number	Enter Layer 3 interface configuration mode.
3	Alpha-A28E(config-if)# ip address ip-address [ip-mask] [vlan-id] Alpha-A28E(config-if)# quit	Configure the IP address for the A10E/A28E and bind the VLAN of specified ID. This VLAN is used to open the Telnet service interface.
4	Alpha-A28E(config)# telnet-server accept port-list { all port-list }	(Optional) configure the interface in support of Telnet function.
5	Alpha-A28E(config)# telnet-server close terminal-telnet session-number	(Optional) release the specified Telnet connection.
6	Alpha-A28E(config)# telnet-server max-session session-number	(Optional) configure device supports maximal Telnet sessions.

- Telnet Client: when you connect the A10E/A28E through the PC terminal emulation program or Telnet client program on a PC, then telnet other A10E/A28E and configure/manage them. As shown in Figure 1-4, Switch A not only acts as Telnet server but also provides Telnet client service.

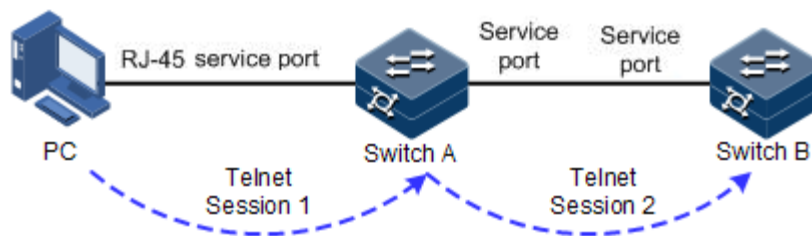


Figure 1-4 A10E/A28E as Telnet client networking

Configure Telnet Client device as below.

Step	Configuration	Description
1	Alpha-A28E# telnet ip-address [port port-id]	Log in to a device from Telnet.

1.1.4 Accessing from SSHv2

Telnet is lack of security authentication and it transports packet by Transmission Control Protocol (TCP) which exists with big potential security hazard. Telnet service may cause hostile attacks, such as Deny of Service (DoS), host IP deceive, and routing deceiving.

The traditional Telnet and File Transfer Protocol (FTP) transmits password and data in plaintext cannot satisfy users' security demands. SSHv2 is a network security protocol, which can effectively prevent the disclosure of information in remote management through data

encryption, and provides greater security for remote login and other network services in network environment.

SSHv2 allows data to be exchanged via TCP and it builds up a secure channel over TCP. Besides, SSHv2 supports other service ports besides standard port 22, thus to avoid illegal attack from network.


Before accessing the A10E/A28E via SSHv2, you must log in to the A10E/A28E through Console interface and starts up SSHv2 service.

The default configuration to accessing the A10E/A28E through SSHv2 is as follows.

Function	Default value
SSHv2 server function status	Disable
Local SSHv2 key pair length	512 bits
SSHv2 authentication method	password
SSHv2 authentication timeout	600s
Allowable failure times for SSHv2 authentication	20
SSHv2 snooping port number	22
SSHv2 session function status	Enable

Configure SSHv2 service for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# generate ssh-key [length]	Generate local SSHv2 key pair and designate its length.
3	Alpha-A28E(config)# ssh2 server	(Optional) start the SSHv2 server. Use the no ssh2 server command to shut down the SSHv2 server.
4	Alpha-A28E(config)# ssh2 server authentication { password rsa-key }	(Optional) configure SSHv2 authentication mode.
5	Alpha-A28E(config)# ssh2 server authentication public-key	(Optional) type the public key of clients to the A10E/A28E in rsa-key authentication mode.
6	Alpha-A28E(config)# ssh2 server authentication-timeout period	(Optional) configure SSHv2 authentication timeout. The A10E/A28E refuses to authenticate and then closes the connection when the client authentication time exceeds this overtemperature threshold.

Step	Configuration	Description
7	Alpha-A28E(config)#ssh2 server authentication- retries <i>times</i>	(Optional) configure the allowable failure times for SSHv2 authentication. The A10E/A28E refuses to authenticate and then closes the connection when client authentication failure numbers exceeds this overtemperature threshold.
8	Alpha-A28E(config)#ssh2 server port <i>port-id</i>	(Optional) configure SSHv2 snooping port number.  Note When configuring SSHv2 snooping port number, the input parameter cannot take effect until SSHv2 is restarted.
9	Alpha-A28E(config)#ssh2 server session session-list enable	(Optional) enable SSHv2 session on the A10E/A28E.

1.1.5 Checking configurations

Use the following commands to check the configuration results.

No.	Configuration	Description
1	Alpha-A28E#show telnet-server	Show configurations of the Telnet server.
2	Alpha-A28E#show ssh2 public-key [authentication rsa]	Show the public key used for SSHv2 authentication on the A10E/A28E and client.
3	Alpha-A28E#show ssh2 { server session }	Show SSHv2 server or session information.

1.2 CLI

1.2.1 Introduction

CLI is the path for communication between user and the A10E/A28E. You can complete device configuration, monitor and management by executing relative commands.

You can log in to the A10E/A28E through PC that run terminal emulation program or the CPE device, enter into CLI once the command prompt appears.

The features of CLI:

- Local configuration via Console interface is available.

- Local or remote configuration via Telnet, Secure Shell v2 (SSHv2) is available.
- Protection for different command levels, users in different level can only execute commands in related level.
- Different command types belong to different command modes. You can only execute a type of configuration in its related command mode.
- You can operate the commands by shortcut keys.
- You can view or execute a historical command by transferring history record. The A10E/A28E supports saving the latest 20 historical commands.
- Online help is available by inputting "?" at any time.
- Smart analysis methods such as incomplete matching and context association, etc. facilitate user input.

1.2.2 Command line level

The A10E/A28E uses hierarchy protection methods to divide command line into 16 levels from low to high.

- 0–4: visitor, users can execute the commands of **ping**, **clear**, and **history**, etc. in this level;
- 5–10: monitor, users can execute the command of **show** and so on;
- 11–14: operator, users can execute commands for different services like VLAN, IP, etc.;
- 15: administrator, used for system basic running commands.

1.2.3 Command line mode

Command line mode is the CLI environment. All system commands are registered in one (or some) command line mode, the command can only run under the corresponding mode.

Establish a connection with the A10E/A28E. If the A10E/A28E is in default configuration, it will enter user EXEC mode, and the screen will display:

```
Alpha-A28E>
```

Input the **enable** command and correct password, and then enter privileged EXEC mode. The default password is admin.

```
Alpha-A28E>enable  
Password:  
Alpha-A28E#
```

In privileged EXEC mode, input the command of **config terminal** to enter global configuration mode.

```
Alpha-A28E#config terminal  
Alpha-A28E(config)#
```

 **Note**

- Command line prompt "Alpha-A28E" is the default host name. You can use the command of **hostname** *string* to modify the host name in privileged EXEC mode.
- Some commands can be used both in global configuration mode and other modes, but the accomplished functions are closely related to command line modes.
- Generally, in a command line mode, you can go back to the previous level command line mode by the command of **quit** or **exit**, but in the privileged EXEC mode, you need to use **disable** command to go back to user EXEC mode.
- Users can go back to privileged EXEC mode through the **end** command from any command line mode except the user EXEC mode or privileged EXEC mode.

The A10E/A28E supports the following command line modes:

Mode	Enter method	Description
User EXEC	Log in to the A10E/A28E, input correct username and password	Alpha-A28E>
Privileged EXEC	In user EXEC mode, input the enable command and correct password.	Alpha-A28E#
Global configuration	In privileged EXEC mode, input the config terminal command.	Alpha-A28E(config)#
Physical layer interface configuration	In global configuration mode, input the interface port <i>port-id</i> command.	Alpha-A28E(config-port)#
Layer 3 interface configuration	In global configuration mode, input the interface ip <i>if-number</i> command.	Alpha-A28E(config-ip)#
VLAN configuration	In global configuration mode, input the vlan <i>vlan-id</i> command.	Alpha-A28E(config-vlan)#
Traffic classification configuration	In global configuration mode, input the class-map <i>class-map-name</i> command.	Alpha-A28E(config-cmap)#
Traffic policy configuration	In global configuration mode, input the policy-map <i>policy-map-name</i> command.	Alpha-A28E(config-pmap)#
Traffic policy configuration binding with traffic classification	In traffic policy configuration mode, input the class-map <i>class-map-name</i> command.	Alpha-A28E(config-pmap-c)#
Access control list configuration	In global configuration mode, input the access-list-map <i>acl-number</i> { deny permit } command.	Alpha-A28E(config-aclmap)#

Mode	Enter method	Description
Service instance configuration	In global configuration mode, input the service <i>cid</i> level <i>level</i> command.	Alpha-A28E(config-service)#
MST region configuration	In global configuration mode, input the spanning-tree region-configuration command.	Alpha-A28E(config-region)#
Profile configuration	In global configuration mode, input the igmp filter profile <i>profile-number</i> command.	Alpha-A28E(config-igmp-profile)#
Cluster configuration	In global configuration mode, input the cluster command.	Alpha-A28E(config-cluster)#

1.2.4 Command line shortcuts

The A10E/A28E supports the following command line shortcuts:

Shortcut	Description
Up cursor key (↑)	Show previous command if there is any command input earlier; the display has no change if the current command is the earliest one in history records.
Down cursor key (↓)	Show next command if there is any newer command; the display has no change if the current command is the newest one in history records.
Left cursor key (←)	Move the cursor one character to left; the display has no change if the cursor is at the beginning of command.
Right cursor key (→)	Move the cursor one character to right; the display has no change if the cursor is at the end of command.
Backspace	Delete the character before the cursor; the display has no change if the cursor is at the beginning of command.
Tab	<p>Click Tab after inputting a complete keyword, cursor will automatically appear a space to the end; click Tab again, the system will show the follow-up inputting keywords.</p> <p>Click Tab after inputting an incomplete keyword, system automatically executes partial helps:</p> <ul style="list-style-type: none"> • System take the complete keyword to replace input if the matched keyword is the one and only, and leave one word space between the cursor and end of keyword; • In case of mismatch or matched keyword is not the one and only, display prefix at first, then click Tab to check words circularly, no space from cursor to the end of keyword, click Space key to input the next word; • If input incorrect keyword, click Tab will change to the next line and prompt error, the input keyword will not change.

Shortcut	Description
Ctrl+A	Move the cursor to the head of line.
Ctrl+C	Break off some running operation, such as ping, traceroute and so on.
Ctrl+D or Delete	Delete the cursor location characters
Ctrl+E	Move the cursor to the end of line.
Ctrl+K	Delete all characters behind the cursor (including cursor location).
Ctrl+X	Delete all characters before the cursor (except cursor location).
Ctrl+Z	Return to privileged EXEC mode from other modes (except user EXEC mode).
Space or y	When the terminal printing command line information exceeds the screen, continue to show the information in next screen.
Enter	When the terminal printing command line information exceeds the screen, continue to show the information in next line.

1.2.5 Command line help message

Complete help

You can get complete help in the below three conditions:

- Click "?" in any command mode to get all commands and their brief description under the command view.

Alpha-A28E>?

The command output is as below.

```
clear      Clear screen
enable    Turn on privileged mode command
exit      Exit current mode and down to previous mode
help      Message about help
history   Most recent historical command
language  Language of help message
list      List command
quit      Exit current mode and down to previous mode
terminal  Configure terminal
test      Test command .
```

- Input a command and followed by a "?" after one character space, if the position of "?" is keyword, list all keyword and brief description.

Alpha-A28E(config)#ntp ?

The command output is as below.

```
peer          Configure NTP peer
refclock-master Set local clock as reference clock
server        Configure NTP server
```

- Input a command and followed by a "?" after one character space, if the position of "?" is parameter, list the range and brief description.

Alpha-A28E(config)#interface ip ?

The command output is as below.

```
<0-14> IP interface number
```

Partial help

You can get partial help in the below three conditions:

- Input a character string and start with a "?", the A10E/A28E will list all keywords starting with the character string under current mode.

Alpha-A28E(config)#c?

The command output is as below.

```
class-map      Set class map
clear          Clear screen
console-cli    Console CLI
cpu            Configure cpu parameters
create         Create static VLAN
```

- Input a command and followed by a character string with "?", the A10E/A28E will list all keywords start with the character string in the command of current mode.

Alpha-A28E(config)#show li?

The command output is as below.

```
link-admin-status link administrator status
link-state-tracking Link state tracking
```

- Input the first few letters of a command keyword and click **Tab** to show complete keyword. The precondition is the input letters can identify the keyword clearly, otherwise, different keywords will be shown circularly after click **Tab**, you can choose the right keyword from them.

Error prompt message

The A10E/A28E prints out the following error prompt according to error type when you input incorrect commands.

Shortcut	Description
% " * " Incomplete command..	User inputs incomplete command.
% Invalid input at '^' marked.	Keyword marked "^" are invalid or do not exist.
% Ambiguous input at '^' marked, follow keywords match it.	Keyword marked with "^" is not clear.
% Unconfirmed command.	The command line input by the user is not unique.
% Unknown command.	The command line input by the user does not exist.
% You Need higher priority!	The user does not have enough right to execute the command line.



Note

If there is error prompt message mentioned above, please use the command line help message to solve the problem.

1.2.6 CLI message

Displaying characteristics

CLI provides the following display characteristics:

- The help message and prompt message in CLI are displayed in both Chinese and English languages.

- Provide pause function when one time display message exceeds one screen, you have the following options at this time, as shown below.

Table 1-1 Function keys description for command line message display characteristics

Function key	Description
Press Space or y	Continue to display next screen message
Press Enter	Continue to display next line message
Press any letter key (except y)	Stop the display and command execution

Filtering displayed information

The A10E/A28E supports a series commands starting with **show**, for checking device configuration, operation and diagnostic information. Generally speaking, these commands can output more information, and then user needs to add filter rules to filter out unnecessary information.

The **show** command of the A10E/A28E supports three kinds of filter modes:

- | **begin string**: show all lines starting from the assigned string;
- | **exclude string**: show all lines mismatch with the assigned string;
- | **include string**: show all lines only match with the assigned string.

Terminal page-break

Terminal page-break refers to the pause function when displayed message exceeds one screen, you can use the display function keys in Table 1-1 to control message display. If message page-break is disabled, it will not provide pause function when displayed message exceeds one screen; all the messages will be displayed circularly at one time.

By default, terminal page-break is enabled.

Configure the A10E/A28E as below.

Step	Configuration	Description
1	A1pha-A28E# terminal page-break enable	Enable display message page-break function

1.2.7 Command line history message

Command line interface can save the user historical command automatically; you can use the up cursor key (↑) or down cursor key (↓) to call the historical command saved by command line repeatedly at any time.

By default, the system saves the recent 20 historical commands in the cache. You can set the number of system stored historical command.

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E> terminal history number	(Optional) configure the number of system stored historical command.
2	Alpha-A28E> terminal time-out period	(Optional) configure the Console terminal timeout period.
3	Alpha-A28E> enable	Enter privileged EXEC mode.
4	Alpha-A28E# history	Show historical commands input by the user.
5	Alpha-A28E# show terminal	Show terminal configurations by the user.

1.2.8 Restoring default value of command line

The default value of command line can be restored by **no** format or **enable | disable** format.

- **no** option: providing in the front of command line to restore the default value, disable some function, delete some setting, etc.; perform some operations opposite to command itself. Commands with **no** option are also known as reverse commands.
- **enable | disable** option: providing in the back or center of command line; **enable** is to enable some feature or function, while **disable** is to prohibit some feature or function.

For example:

- Perform description text command in physical layer interface mode to modify the interface description; perform no description command to delete the interface description and restore the default values.
- Use the **shutdown** command in physical layer interface mode to disable an interface; use the **no shutdown** command to enable an interface.
- Use the **shutdown** command in global configuration mode to disable an interface; use the **no shutdown** to enable an interface.
- Use the **terminal page-break enable** command in global configuration mode to enable terminal page-break; use the **terminal page-break disable** command to disable terminal page-break.



Note

Most configuration commands have default values, which often are restored by **no** option.

1.3 Managing users

When you start the A10E/A28E for the first time, connect the PC through Console interface to the A10E/A28E, input the initial user name and password in HyperTerminal to log in and configure the A10E/A28E.



Note

Initially, both the user name and password are admin

If there is not any privilege restriction, any remote user can log in to the A10E/A28E via Telnet or access network by building Point to Point Protocol (PPP) connection when the Simple Network Management Protocol (SNMP) interface or other service interface of the A10E/A28E are configured with IP address. This is unsafe to the A10E/A28E and network. Creating user for the A10E/A28E and setting password and privilege help manage the login users and ensures network and device security.

Configure login user management for the A10E/A28E of as below.

Step	Configuration	Description
1	Alpha-A28E# user name <i>user-name</i> password <i>password</i>	Create or modify the user name and password.
2	Alpha-A28E# user name <i>user-name</i> privilege <i>privilege-level</i>	Configure login user privilege. The initial user privilege is 15, which is the highest privilege.
3	Alpha-A28E# user <i>user-name</i> { allow-exec disallow-exec } <i>first-keyword</i> [<i>second-keyword</i>]	Configure the priority rule for login user to perform the command line. Specified allow-exec parameters will allow the user to perform commands higher than the current priority. Specified disallow-exec parameter will allow the user to perform commands lower than the current priority only.

1.3.1 Checking configurations

Use the following commands to check configuration results.

No.	Configuration	Description
1	Alpha-A28E# show user [detail]	Show information about the login users

1.4 Managing files

1.4.1 Managing BootROM files

The BootROM file is used to boot the A10E/A28E and finish device initialization. You can upgrade the BootROM file through File Transfer Protocol (FTP) FTP or Trivial File Transfer Protocol (TFTP). By default, the name of the BootROM file is bootrom or bootromfull.

After powering on the A10E/A28E, run the BootROM files at first, click **Space** to enter BootROM menu when the prompt "Press space into Bootrom menu..." appears:

```
begin...
ram size: 64M DDR testing...done
File System Version:1.0

Init flash ...Done

Bootstrap_3.1.6.Alpha-A28E.1.20130729, Orion Networks Compiled Jul 29
2013, 18:37:36
Base Ethernet MAC address: f8:f0:82:99:99:99

Press space into Bootstrap menu...
4
```

In Boot mode, you can do the following operations.

Operation	Description
?	List all executable operations.
b	Quick execution for system bootrom software.
E	Format the memory of the A10E/A28E.
h	List all executable operations.
u	Download the system startup file through the XMODEM.
N	Set Medium Access Control (MAC) address.
R	Reboot the A10E/A28E.
T	Download the system startup software through TFTP and replace it.
V	Show device BootROM version.

System files are the files needed for system operation (like system startup software, configuration file). These files are usually saved in the memory, the A10E/A28E manages them by a file system to facilitate user manage the memory. The file system contains functions of creating, deleting and modifying file and directory.

Besides, the A10E/A28E supports dual system; that is to say, it can store two versions of system software in memory. You can shift to the other version when one version cannot work due to system upgrade failure.

Configure system files management for the A10E/A28E as below.

All the following steps are optional and no sequencing.

Step	Configuration	Description
1	<code>A1pha-A28E#download bootstrap { ftp ip-address user-name password file-name tftp ip-address file-name }</code>	(Optional) download the BootROM file through FTP or TFTP.

Step	Configuration	Description
2	Alpha-A28E# download system-boot { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	(Optional) download the system startup file through FTP or TFTP.
3	Alpha-A28E# upload system-boot { ftp [<i>ip-address user-name password file-name</i>] tftp [<i>ip-address file-name</i>] }	(Optional) upload the system startup file through FTP or TFTP.
4	Alpha-A28E# erase [<i>file-name</i>]	(Optional) delete files saved in the memory.

1.4.2 Managing system files

Configuration files are loaded after starting the system; different files are used in different scenarios in order to achieve different service functions. After starting the system, you can configure the A10E/A28E and save the configuration files. New configuration will take effect in next boot.

Configuration file has an affix ".cfg", and these files can be open by text book program in Windows system. The contents in the following format:

- Saved as Mode+Command format;
- Just reserve the non-defaulted parameters to save space (refer to command reference for default values of configuration parameters);
- Take the command mode for basic frame to organize commands, put commands of one mode together to form a section, the sections are separated by "!".

The A10E/A28E starts initialization by reading configuration files from memory after powering on. Thus, the configuration in configuration files are called initialization configuration. If there is no configuration files in memory, the A10E/A28E takes the default parameters for initialization.

The configuration that is currently used by the A10E/A28E is called running configuration.

You can modify the A10E/A28E current configuration through command line. The current configuration can be used as initial configuration when next time power on, user must use the **write** command to save current configuration into memory and form configuration file.

Configure the configuration files management for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# download system [master slave] { ftp <i>ip-address user-name password file-name</i> sftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	(Optional) download the system boot file through FTP or TFTP.
2	Alpha-A28E# erase [<i>file-name</i>]	(Optional) delete files saved in the flash.

Step	Configuration	Description
3	Alpha-A28E# upload system [master slave] { ftp <i>ip-address user-name password file-name</i> sftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	(Optional) upload the system boot file through FTP or TFTP.

1.4.3 Managing configuration files

Configuration files are loaded after starting the system; different files are used in different scenarios in order to achieve different service functions. After starting the system, you can configure the A10E/A28E and save the configuration files. New configuration will take effect in next boot.

Configuration file has an affix ".cfg", and these files can be opened by text program in Windows system. The contents in the following format:

- Saved as Mode+Command format.
- Just reserve the non-defaulted parameters to save space (refer to command reference for default values of configuration parameters).
- Take the command mode for basic frame to organize commands, put commands of one mode together to form a section, the sections are separated by "!".

The A10E/A28E starts initialization by reading configuration files from memory after powering on. Thus, the configuration in configuration files are called initial configuration. If there is no configuration files in memory, the A10E/A28E take the default parameters for initialization.

The configuration that is currently used by the A10E/A28E is called running configuration.

You can modify the A10E/A28E current configuration through CLI. The running configuration can be used as initial configuration when next time power on, you must use command **write** to save current configuration into memory and form configuration file.

Configure the configuration files management for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# download startup-config { ftp [<i>ip-address user-name password file-name</i>] [reservedevcfg] tftp [<i>ip-address file-name</i>] [reservedevcfg] }	(Optional) download the startup configuration file through FTP or TFTP.
2	Alpha-A28E# erase [<i>file-name</i>]	(Optional) delete files saved in the memory.
3	Alpha-A28E# upload startup-config { ftp [<i>ip-address user-name password file-name</i>] tftp [<i>ip-address file-name</i>] }	(Optional) upload the startup configuration file through FTP or TFTP.
4	Alpha-A28E# write	(Optional) save the running configuration file into the memory.

1.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show startup-config [<i>file-name</i>]	Show configuration information loaded upon device startup.
2	Alpha-A28E# show running-config [interface port [<i>port-id</i>]]	Show the running configuration information.

1.5 Configuring clock management

1.5.1 Configuring time and time zone

To ensure the A10E/A28E to work well with other devices, you must configure system time and belonged time zone accurately.

The A10E/A28E supports three types of system time mode, which are time stamp mode, auxiliary time mode, and default mode from high to low according to timing unit accuracy. You need to select the most suitable system time mode by manual in accordance with actual application environment.

The default configuration of time and time zone is as below.

Function	Default value
System time	2000-01-01 08:00:00.000
System clock mode	default
System belonged time zone	UTC+8
Time zone offset	+08:00
Functional status of Daylight Saving Time	Disable

Configure time and time zone for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# clock set <i>hour minute second year month day</i>	Configure system time.
2	Alpha-A28E# clock timezone { + - } <i>hour minute timezone-name</i>	Configure system belonged time zone.
3	Alpha-A28E# clock mode { auxiliary default timestamp }	Configure system clock mode.

1.5.2 Configuring DST

Daylight Saving Time (DST) is a kind of artificial regulation local time system for saving energy. At present, there are nearly 110 countries operating DST every summer around the world, but different countries have different stipulations for DST. Thus, you should consider the local conditions when configuring DST.

Configure DST for the A10E/A28E as below.

Step	Configuration	Description
1	<code>Alpha-A28E#clock summer-time enable</code>	Enable DST. Use the clock summer-time disable command to disable this function.
2	<code>Alpha-A28E#clock summer-time recurring { week last } { fri mon sat sun thu tue wed } month hour minute { week last } { fri mon sat sun thu tue wed } month hour minute offset-mm</code>	Configure calculation period for system DST.



Note

- When you set system time manually, if the system uses DST, such as DST from 2 a.m. on the second Sunday, April to 2 a.m. on the second Sunday, September every year, you have to advance the clock one hour faster during this period, set time offset as 60 minutes and from 2 a.m. to 3 a.m. on the second Sunday, April each year is an inexistent time. The time setting by manual operation during this period shows failure.
- The summer time in southern hemisphere is opposite to northern hemisphere, which is from September to April of next year. If user configures start time later than ending time, system will suppose it is in the Southern Hemisphere. That is to say, the summer time is the start time this year to the ending time of next year.

1.5.3 Configuring NTP

Network Time Protocol (NTP) is a time synchronization protocol defined by RFC1305, used to synchronize time between distributed time servers and clients. NTP transportation is based on UDP, using port 123.

The purpose of NTP is to synchronize all clocks in a network quickly and then the A10E/A28E can provide different application over a unified time. Meanwhile, NTP can ensure very high accuracy, with accuracy of 10ms around.

The A10E/A28E in support of NTP cannot only accept synchronization from other clock source, but also to synchronize other devices as a clock source.

The A10E/A28E adopts multiple NTP working modes for time synchronization:

- Server/Client mode

In this mode, client sends clock synchronization message to different servers. The server works in server mode by automation after receiving synchronization message and send

answering message. The client received answering message and perform clock filer and selection, then synchronize it to privileged server.

In this mode, client can synchronize to server but the server cannot synchronize to client.

- Symmetric peer mode

In this mode, active equity send clock synchronization message to passive equity. The passive equity works in passive mode by automation after receiving message and send answering message back. By exchanging messages, the two sides build up symmetric peer mode. The active and passive equities in this mode can synchronize each other.

The NTP default configuration is as below.

Function	Default value
Whether the A10E/A28E is NTP master clock	no
Global NTP server	inexistent
Global NTP equity	inexistent
Reference clock source	0.0.0.0

Configure NTP for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ntp server <i>ip-address</i> [version [v1 v2 v3]]	(Optional) configure NTP server address for client device working in server/client mode.
3	Alpha-A28E(config)# ntp peer <i>ip-address</i> [version [v1 v2 v3]]	(Optional) configure NTP equity address for the A10E/A28E working in symmetric peer mode.
4	Alpha-A28E(config)# ntp refclock-master [<i>ip-address</i>] [<i>stratum</i>]	Configure clock of the A10E/A28E as NTP reference clock source for the A10E/A28E.



Note

If the A10E/A28E is configured as NTP reference clock source, the NTP server or NTP equity are not configurable; and vice versa, the A10E/A28E cannot be configured as NTP reference clock if the NTP server or equity are configured.

1.5.4 Configuring SNTP

Simple Network Time Protocol (SNTP) is mainly used to synchronize Switch system time with the SNTP device time in the network. The time synchronized by SNTP protocol is Greenwich Mean Time (GMT), which can be changed to local time according to system setting of time zone.

The SNTP default configuration is as below.

Function	Default value
SNTP server address	inexistent

Configure SNTP for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# sntp server ip-address	(Optional) configure the IP address of the SNTP server which works in server/client mode.



Note

After configuring SNTP server address, the A10E/A28E will try to get clock information from SNTP server every 3s, and the maximum timeout for clock information is 10s.

1.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show clock [summer-time-recurring]	Show the A10E/A28E system time, time zone and DST configuration.
2	Alpha-A28E# show sntp	Show SNTP configurations.
3	Alpha-A28E# show ntp status	Show NTP configurations.
4	Alpha-A28E# show ntp associations [detail]	Show NTP connection information.

1.6 Configuring interface management

1.6.1 Default configurations of interfaces

The default configuration of physical layer interface is as below.

Function	Default value
Maximum forwarding frame length of interface	9712 Bytes
Duplex mode of interface	Auto-negotiation

Function	Default value
Interface speed	Auto-negotiation
Interface flow control status	Disable
Optical/Electrical mode of the Combo interface	Automatical
Flow control of the Combo interface	Disable
Time interval of interface dynamic statistics	2s
Interface status	Enable

1.6.2 Configuring basic attributes for interfaces

The interconnected devices cannot communicate normally if their interface attributes (such as MTU, duplex mode, and speed) are inconsistent, and then you have to adjust the interface attribute to make the devices at both ends match each other.

Configure the basic attributes for interface of the A10E/A28E.

Step	Configuration	Description
1	<code>Alpha-A28E#config</code>	Enter global configuration mode.
2	<code>Alpha-A28E(config)#interface port <i>port-id</i></code>	Enter physical layer interface configuration mode.
3	<code>Alpha-A28E(config-port)#flowcontrol { off on }</code>	Enable/Disable flow control of 802.3x packets on the interface.

1.6.3 Configuring flow control on interfaces

IEEE802.3x is flow control of full-duplex Ethernet data layer. Then the client sends request to the server; the client sends PAUSE frame to server if there is system or network jam, so it delays data transmission from server to client.

Configure flow control for the A10E/A28E as below.

Step	Configuration	Description
1	<code>Alpha-A28E#config</code>	Enter global configuration mode.
2	<code>Alpha-A28E(config)#interface port <i>port-id</i></code>	Enter physical layer interface configuration mode.
3	<code>Alpha-A28E(config-port)#flowcontrol { off on }</code>	Enable/Disable flow control over 802.3x packet on the interface.

1.6.4 Configuring the Combo interface

The A10E/A28E Combo interface supports both optical module and electrical module, so transmission media can be optical fiber or cable according to interface media type supported by the peer device. If using both two kinds of transmission media for connection, service transmission can only use one of them at the same time.

The Combo interface has two modes to select transmission media: mandatory and automatic. If the configuration mode is automatic selection and two kinds of transmission medium of optical fiber and cable connections are normal, the interface will automatically choose one of them as an effective transmission line as well as automatically select another transmission medium for service transmission when current transmission medium breaks down.

In auto-selection mode, after the Combo optical interface and Combo electrical interface are configured respectively, the device automatically use the optical/electrical interface if needed, without configuring them every time upon use.

Configure the Combo interface for the A10E/A28E as below.

Step	Configuration	Description
1	<code>Alpha-A28E#config</code>	Enter global configuration mode.
2	<code>Alpha-A28E(config)#interface port <i>port-id</i></code>	Enter physical layer interface configuration mode.
3	<code>Alpha-A28E(config-port)#media-priority { fiber copper }</code>	Configure Combo interface optical/electrical priority. Optical/electrical priority selection function can select to use optical port or electrical port in prior when inserting optical port or electrical port at the same time.
4	<code>Alpha-A28E(config-port)#description medium-type { fiber copper } <i>word</i></code>	Configure Combo interface optical/electrical description information.
5	<code>Alpha-A28E(config-port)#speed medium-type { fiber copper } { auto 10 100 1000 }</code>	Configure Combo interface optical/electrical transmission speed. The interface speed also depended on the module specification used.
6	<code>Alpha-A28E(config-port)#duplex medium-type copper { full half }</code>	Configure Combo interface electrical duplex mode.
7	<code>Alpha-A28E(config-port)#mdi medium-type copper { auto normal across }</code>	Configure Combo interface as electrical port MDI mode.
8	<code>Alpha-A28E(config-port)#flowcontrol medium-type { fiber copper } { on off }</code>	Configure Combo interface optical/electrical flow control.

1.6.5 Configuring interface rate statistics

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# sfp detect-mode { auto-detect force-100base-x force-1000base-x }	Configure SFP interface detection mode. Non-SFP interfaces cannot be configured with detection mode.

1.6.6 Configuring interface statistics

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# dynamic statistics time <i>period</i>	Configure period for interface dynamic statistics. By default, it is 2s.
3	Alpha-A28E(config)# clear interface port <i>port-id</i> statistics	Clear interface statistics saved on the A10E/A28E.

1.6.7 Enabling/Disabling interfaces

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# shutdown	Disable current interface. Use the command of no shutdown to re-open the closed interface.

1.6.8 Checking configurations


Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show interface port [<i>port-id</i>]	Show interface status.

No.	Item	Description
2	Alpha-A28E# show interface port <i>port-id</i> statistics dynamic [detail]	Show interface statistics.
3	Alpha-A28E# show interface port [<i>port-id</i>] flowcontrol	Show flow control on the interface.
4	Alpha-A28E# show system mtu	Show system MTU.
5	Alpha-A28E# show combo description port [<i>port-id</i>]	Show information about the Combo interface.
6	Alpha-A28E# show combo configuration port [<i>port-id</i>]	Show configurations of the Combo interface.
7	Alpha-A28E# show sfp detect-mode port [<i>port-id</i>]	Show detection mode of the SFP interface.

1.7 Configuring basic information

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# hostname <i>name</i>	(Optional) configure device name. By default, the device name is Alpha-A28E. The system supports changing device name to make users distinguish different devices in the network. Device name become effective immediately, which can be seen in terminal prompt.
2	Alpha-A28E# language { chinese english }	(Optional) configure switchover language mode. By default, the language is English. The system supports displaying help and prompt information is both English and Chinese.
3	Alpha-A28E# write	Save configuration. Save configuration information to the A10E/A28E after configuration, and the new saved configuration information will cover the original configuration information. Without saving, the new configuration information will lose after rebooting, and the A10E/A28E will continue working with the original configuration.  Caution Use the command of erase file-name to delete the configuration file. This operation cannot be restored, so use this command with care.

Step	Configuration	Description
4	Alpha-A28E# reboot [now]	(Optional) configure reboot options. When the A10E/A28E is in failure, please reboot it to solve the problem according to actual condition.
5	Alpha-A28E# erase [<i>file-name</i>]	(Optional) delete files saved in the memory.

1.8 Task scheduling

When you need to use some commands periodically or at a specified time, configure task scheduling.

The A10E/A28E supports realizing task scheduling by combining the program list to command line. You just need to designate the task start time, period and end time in the program list, and then bind the program list to command line so as to realize the periodic operation of command line.

Configure task scheduling for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# schedule-list <i>list-number</i> start { <i>date-time</i> <i>month-day-year</i> <i>hour:minute:second</i> [every { day week <i>period</i> <i>hour:minute:second</i> }] stop <i>month-day-year</i> <i>hour:minute:second</i> up-time <i>period</i> <i>hour:minute:second</i> [every <i>period</i> <i>hour:minute:second</i>] [stop <i>period</i> <i>hour:minute:second</i>] }	Create and configure schedule list.
3	Alpha-A28E(config)# <i>command-string</i> schedule-list <i>list-number</i>	Bind the command line which needs periodic execution and supports schedule list to the schedule list.
4	Alpha-A28E# show schedule-list [<i>list-number</i>]	Show configurations of the schedule list.

1.9 Watchdog

The interference of outside electromagnetic field will influence the working of single chip microcomputer, and cause program fleet and dead circulation so that the system cannot work normally. Considering the real-time monitoring to the running state of single chip

microcomputer, it generates a program specially used to monitoring the running status of switch hardware, which is commonly known as the Watchdog.

The system will reboot when the Switch cannot continue to work for task suspension or dead circulation, and without feeding the dog within a feeding dog cycle.

The watchdog function configuration can prevent the system program from dead circulation caused by uncertainty fault so as to improve the stability of system.

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# watchdog enable	Enable watchdog.
2	Alpha-A28E# show watchdog	Show watchdog status.

1.10 Load and upgrade

1.10.1 Introduction

Load

In traditional, configuration files are loaded by serial port, it takes a long time to load for the low speed and remote loading is unavailable. FTP and TFTP loading modes can solve those problems and make operation more convenient.

The A10E/A28E supports TFTP auto-loading mode.

TFTP auto-loading means users get the device configuration files from server and then configure the device. Auto-loading function allows configuration files to contain loading related commands for multiple configurations loading so as to meet file auto-loading requirements in complex network environment.

The A10E/A28E provides several methods to confirm configuration file name in TFTP server, such as input by manual, obtain by DHCP Client, use default configuration file name, etc. Besides, users can assign certain denomination rule for configuration files and then, the device confirms the name according to the rules and combines with itself attribution (device type, MAC address, software version, and so on).

Upgrade

The A10E/A28E needs to upgrade if you want to add new features, optimize functions or solve current software version bugs.

The A10E/A28E supports the following two upgrade modes:

- Upgrade by BootROM
- Upgrade by command line

1.10.2 Configuring TFTP auto-upload method

You need to build TFTP environment before configuring TFTP auto-upload method to have the A10E/A28E interconnect with TFTP server.



Note

- When you perform configuration auto-loading function, the IP address priority configured by commands is higher than the one obtained by DHCP Client.
- When you perform configuration auto-loading function, configuration file name obtained from server in priority turn from higher to lower as file name confirmed by naming convention > file name configured by command > file name obtained by DHCP Client.

Configure TFTP auto-loading for the A10E/A28E as below.

No.	Item	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# service config tftp-server ip-address	Configure the IP address of the TFTP server. By default, this address is not configured.
3	Alpha-A28E(config)# service config filename rule [rule-number]	Set naming convention rule for file name. By default, there is no naming convention, and the system uses default file name as startup_config.conf .
4	Alpha-A28E(config)# service config filename file-name	Specify the name of the configuration file to be uploaded.
5	Alpha-A28E(config)# service config version { system-boot bootstrap startup-config } version	Configure file version No.
6	Alpha-A28E(config)# service config overwrite enable	Enable local configuration file overwriting.
7	Alpha-A28E(config)# service config	Enable configuration auto-loading.
8	Alpha-A28E(config)# service config trap enable	Enable Trap function.

1.10.3 Upgrading system software by BootROM

In the below conditions, user needs to upgrade system software by BootROM:


- The device is started for the first time.
- A system file is damaged.


- The card cannot start up in order.

Before upgrading system software by BootROM, you should build FTP environment, take the PC as FTP server and the A10E/A28E as client. Basic requirements are as below.

- Configure FTP server, make sure the server is available.
- Configure IP address for TFTP server; keep it in the same network segment with A10E/A28E IP address.

Steps for upgrading system software by BootROM:

Step	Operation
1	<p>Log in device through serial port as administrator and enter Privileged EXEC mode, reboot the A10E/A28E by the command of reboot.</p> <pre>Alpha-A28E#reboot Please input 'yes' to confirm:yes Rebooting ...</pre>
2	<p>Click Space key to enter interface when the display shows "Press space into Bootstrap menu...", then input "?" to display command list:</p> <pre>[Alpha-A28E]:? ? - List all available commands h - List all available commands v - Show bootstrap version b - Boot an executable image E - Format both DOS file systems T - Download system program u - XMODEM download system boot image N - set ethernet address R - Reboot</pre> <div style="text-align: center;">  <p>Caution The input letters are case sensitive.</p> </div>

Step	Operation
3	<p>Input "T" to download system boot file through TFTP. The system displays the following information.</p> <pre data-bbox="491 421 1385 734">[Alpha-A28E]:T dev name:et unit num:1 file name: system_boot.z NOS_4.14.1921.Alpha-A28E.000.20130729 local ip: 192.168.1.1 192.168.18.250 server ip: 192.168.1.2 192.168.18.16 user:wrs 1 password:wrs 123456 Loading... Done Saving file to flash...</pre> <div data-bbox="491 786 730 869" style="text-align: center;">  Caution </div> <p data-bbox="512 875 1385 936">Ensure the input file name here is correct, the file name should not be longer than 80 characters.</p>
4	<p>Input "b" to quick execute bootstrap file. The A10E/A28E will reboot and load the downloaded system boot file.</p>

1.10.4 Upgrading system software by CLI

Before upgrading system software by command line, you should build FTP/TFTP environment, take the PC as FTP/TFTP server and the A10E/A28E as client. Basic requirements are as below.

- The A10E/A28E connects to the TFTP server.
- Configure the FTP/TFTP server. Ensure the server is available.
- Configure IP address for FTP/TFTP server to make sure that A10E/A28E can access the server.

Upgrade system software through CLI as below.

No.	Item	Description
1	Alpha-A28E# download system-boot { ftp [<i>ip-address user-name password file-name</i>] tftp [<i>ip-address file-name</i>] }	Download system boot file through FTP/TFTP.
2	Alpha-A28E# write	Write the configured file into the memory.
3	Alpha-A28E# reboot [now]	Reboot the A10E/A28E, and it will automatically load the downloaded system boot file.

1.10.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show service config	Show auto-configured loading information.
2	Alpha-A28E# show service config filename rule <i>rule-number</i>	Show naming convention for configuration files.
3	Alpha-A28E# show version	Show system version.

1.10.6 Exampe for configuring TFTP auto-loading

Networking requirements

As shown in Figure 1-5, connect the TFTP server with the switch, and configure auto-loading function on the switch to make the switch automatically load configuration file from TFTP server. Hereinto, the IP address of the TFTP server is 192.168.1.1, subnet mask is 255.255.255.0, and the naming convention for configuration file name meets the following conditions:

- Device model is included in configuration file name.
- Complete MAC address is included in configuration file name.
- First 2 digits of software version are included in configuration file name.
- No extension rules are supported.

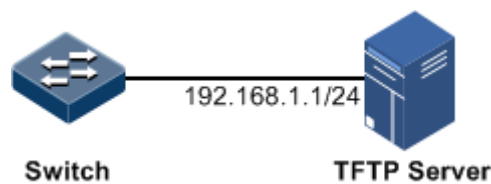


Figure 1-5 Configuring auto-loading

Configuration steps

Step 1 Configure IP address for TFTP server.

```
Alpha-A28E#config
Alpha-A28E(config)#service config tftp-server 192.168.1.1
```

Step 2 Configure naming convention rules.

```
Alpha-A28E(config)#service config filename rule 81650
```

Step 3 Configure file name.

```
Alpha-A28E(config)#service config filename ABC
```

Step 4 Enable local configuration file overwriting.

```
Alpha-A28E(config)#service config overwrite enable
```

Step 5 Enable auto-loading configuration.

```
Alpha-A28E(config)#service config
```

Checking results

View auto-loading configuration by the command of **show service config**.

```
Alpha-A28E#show service config
Auto upgrade :                enable
Config server IP address:     192.168.1.1
Config filename rule:         81650
Config file name:             ABC
System boot file version:     1107290
Bootstrap flie version :     :48:050
Startup-config file version:  0000000
Overwrite local configuration file: enable
Send Completion trap:        disable
Current File Type:            none
Operation states:             done
Result:                        none
```

2 Ethernet

This chapter describes the configuration and principle of Ethernet features, also provides some related configuration instances, including the following chapters:

- MAC address table
- VLAN
- QinQ
- VLAN mapping
- Interface protection
- Port mirroring
- Layer 2 protocol transparent transmission

2.1 MAC address table

2.1.1 Introduction

The MAC address table records mappings between MAC addresses and interfaces. It is the basis for an Ethernet device to forward packets. When the Ethernet device forwards packets on Layer 2, it searches for the forwarding interface according to the MAC address table, implements fast forwarding of packets, and reduces broadcast traffic.

Item of MAC address table contains the below information:

- Destination MAC address
- Destination MAC address related interface ID
- Interface belonged VLAN ID
- Flag bits

The A10E/A28E supports showing MAC address information by device, interface, or VLAN.

MAC address forwarding modes

When forwarding packets, based on the information about MAC addresses, the A10E/A28E adopts following modes:

- Unicast: when a MAC address entry, related to the destination MAC address of a packet, is listed in the MAC address table, the A10E/A28E will directly forward the packet to the receiving port through the egress port of the MAC address entry. If the entry is not listed, the A10E/A28E broadcasts the packet to other devices.
- Multicast: when the A10E/A28E receives a packet of which the destination MAC address is a multicast address, and multicast is enabled, the A10E/A28E sends the packet to the specified Report interface. If an entry corresponding to the destination address of the packet is listed in the MAC address table, the A10E/A28E transmits the packet from the egress port of the entry. If the corresponding entry is not listed, the A10E/A28E broadcasts the packet to other interfaces except the receiving interface.
- Broadcast: when the A10E/A28E receives a packet with an all-F destination address, or its MAC address is not listed in the MAC address table, the A10E/A28E forwards the packet to all ports except the port that receives this packet.

Classification of MAC addresses

MAC address table is divided into static address entry and dynamic address entry.

- Static MAC address entry: also called "permanent address", added and removed by the user manually, does not age with time. For a network with small device change, adding static address entry manually can reduce the network broadcast flow, improve the security of the interface, and prevent table entry from losing after the system is reset.
- Dynamic MAC address entry: the Switch can add dynamic MAC address entry through MAC address learning mechanism. The table entries age according to the configured aging time, and will be empty after the system is reset.

The A10E/A28E supports the maximum 16K dynamic MAC addresses, and each interface supports 1024 static MAC addresses.

Aging time of MAC addresses

There is capacity restriction to the MAC address table of the A10E/A28E. In order to maximize the use of address forwarding table resources, the A10E/A28E uses the aging mechanism to update MAC address table, i.e. in the meantime of creating a certain dynamic table entry, open the aging timer, if there is no MAC address packet from the table entry during the aging time, the A10E/A28E will delete the MAC address entry.

The A10E/A28E supports aging for MAC addresses. The aging time ranges from 10s to 1000000s, and can be 0 which indicates no aging.



The aging mechanism takes effect on dynamic MAC addresses only.

MAC address forwarding policies

The MAC address table has two forwarding policies:

When receiving packets on an interface, the A10E/A28E searches the MAC address table for the interface related to the destination MAC address of packets.

- If successful, it forwards packets on the related interface, records the source MAC address of packets, interface number of ingress packets, and VLAN ID in the MAC

address table. If packets from other interface are sent to the MAC address, the A10E/A28E can send them to the related interface.

- If failed, it broadcasts packets to all interfaces except the source interface, and records the source MAC address in the MAC address table.

MAC address limit

MAC address learning amount limit function is mainly to restrict the number of MAC addresses, avoid extending the checking time of forwarding table entry caused by too large MAC address table and degrading the forwarding performance of Ethernet switch, and it is an effective way to manage MAC address table.

MAC address learning amount limit is mainly used to restrict the size of MAC address table and improve the speed of forwarding packets.

2.1.2 Preparing for configurations

Scenario

Configure static MAC address table in the following situations:

- Static MAC address can be set for fixed server, special persons (manager, financial staff, etc.) fixed and important hosts to make sure all data flow forwarding to these MAC addresses are forwarded from static MAC address related interface in priority.
- For the interface with fixed static MAC address, you can disable MAC address learning to avoid other hosts visiting LAN data from the interface.

Configure aging time for dynamic MAC address table to avoid saving too many MAC address table entries in MAC address table and running out of MAC address table resources so as to achieve dynamic MAC address aging function.

Prerequisite

N/A

2.1.3 Default configurations of MAC address table

The default configuration of MAC address table is as below.

Function	Default value
MAC address learning function status	Enable
MAC address aging time	300s
MAC address limit	Unlimited

2.1.4 Configuring static MAC address

Configure static MAC address as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mac-address-table static unicast <i>mac-address</i> vlan <i>vlan-id</i> port <i>port-id</i>	Configure static unicast MAC addresses.
	Alpha-A28E(config)# mac-address-table static multicast <i>mac-address</i> vlan <i>vlan-id</i> port-list <i>port-list</i>	Configure static multicast MAC addresses.
3	Alpha-A28E(config)# mac-address-table blackhole { destination source } <i>mac-address</i> vlan <i>vlan-id</i>	Configure blackhole MAC addresses.



Note

- The MAC address of the source device, multicast MAC address, FFFF.FFFF.FFFF, and 0000.0000.0000 cannot be configured as static unicast MAC address.
- The maximum number of static unicast MAC addresses supported by the A10E/A28E is 1024.

2.1.5 Configuring multicast filtering mode for MAC address table

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mac-address-table multicast filter-mode { filter-all forward-all filter-vlan <i>vlan-list</i> }	Configure multicast filtering mode of MAC address table.

2.1.6 Configuring MAC address learning

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mac-address-table learning { enable disable } port-list { all <i>port-list</i> }	Enable/Disable MAC address learning.

2.1.7 Configuring MAC address limit

Configuring interface-based MAC address limit

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# mac-address-table threshold <i>threshold-value</i>	Configure interface-based MAC address limit.

2.1.8 Configuring the aging time of MAC addresses

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mac-address-table aging-time { 0 <i>period</i> }	Configure the aging time of MAC addresses. The aging time ranges from 10s to 1000000s, and can be 0 which indicates no aging.

2.1.9 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show mac-address-table static [<i>port port-id</i> <i>vlan vlan-id</i>]	Show static unicast MAC addresses.
2	Alpha-A28E# show mac-address-table multicast [<i>vlan vlan-id</i>] [<i>count</i>]	Show all Layer 2 multicast addresses and the current multicast MAC address number.
3	Alpha-A28E# show mac-address-table l2-address [<i>count</i>] [<i>vlan vlan-id</i> <i>port port-id</i>]	Show all Layer 2 unicast MAC addresses and the current unicast MAC address number.
4	Alpha-A28E# show mac-address-table threshold [<i>port-list port-list</i>]	Show dynamic MAC address limit.
5	Alpha-A28E# show mac aging-time	Show the aging time of dynamic MAC addresses.

2.1.10 Maintenance

Maintain the A10E/A28E as below.

Command	Description
Alpha-A28E(config)# clear mac-address-table { all blackhole dynamic static } [vlan vlan-id]	Clear MAC address.
Alpha-A28E# search mac-address <i>mac-address</i>	Search MAC address.

2.1.11 Example for configuring the MAC address table

Networking requirements

Configure static unicast MAC address for Port 2 on Switch A, and configure the aging time for dynamic MAC addresses (it takes effect only after dynamic MAC address learning is enabled).

As shown in Figure 2-1, configure Switch A as below:

- Create VLAN 10 and activate it.
- Configure a static unicast MAC address 0001.0203.0105 on Port 2 and set its VLAN to VLAN 10.
- Set the aging time to 500s.

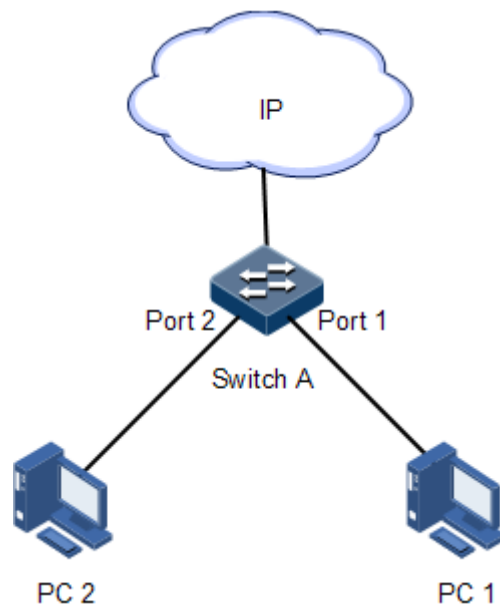


Figure 2-1 MAC application networking

Configuration steps

- Step 1 Create VLAN 10 and active it, and add Port 2 into VLAN 10.

```
Alpha-A28E#config  
Alpha-A28E(config)#create vlan 10 active  
Alpha-A28E(config)#interface port 2  
Alpha-A28E(config-port)#switchport mode access  
Alpha-A28E(config-port)#exit
```

Step 2 Configure a static unicast MAC address on Port 2, and set its VLAN to VLAN 10.

```
Alpha-A28E(config)#mac-address-table static unicast 0001.0203.0405 vlan 10 port 2
```

Step 3 Set the aging time to 500s.

```
Alpha-A28E(config)#mac-address-table aging-time 500
```

Checking results

Show MAC address configuration by the command of **show mac-address-table l2-address port port-id**.

```
Alpha-A28E#show mac-address-table l2-address port 2  
Aging time: 500 seconds  
Mac Address      Port      Vlan      Flags  
-----  
0001.0203.0405  2         10        Static
```

2.2 VLAN

2.2.1 Introduction

Overview

Virtual Local Area Network (VLAN) is a protocol to solve Ethernet broadcast and security problems. It is a Layer 2 isolation technique that divides a LAN into different broadcast domains logically rather than physically, and then the different broadcast domains can work as virtual groups without any influence from one another. As for the function, VLAN has the same features as LAN, but members in one VLAN can access one another without restriction by physical location.

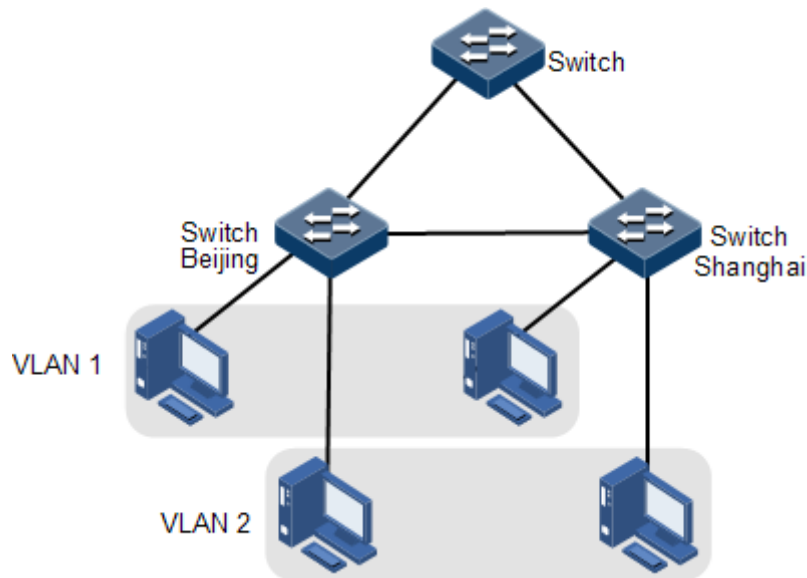


Figure 2-2 Dividing VLANs

VLAN technique can divide a physical LAN into different broadcast domains logically. Hosts without intercommunication requirements can be isolated by VLAN and then, improve network security, reduce broadcast flow and broadcast storm.

The A10E/A28E supports interface-based VLAN division.

The A10E/A28E complies with IEEE 802.1Q standard VLAN and supports 4094 concurrent VLANs.

Interface mode and packet forwarding

The interface modes of the A10E/A28E include Access mode and Trunk mode. The method of dealing with packet for the two modes shows as below.

Table 2-1 Interface mode and packet processing

Interface type	Dealing with ingress packets		Dealing with Egress packet
	Untag packet	Tag packet	
Access	Add Access VLAN Tag for packet.	<ul style="list-style-type: none"> • VLAN ID = Access VLAN ID, receive the packet • VLAN ID ≠ Access VLAN ID, discard the packet. 	<ul style="list-style-type: none"> • VLAN ID = Access VLAN ID, remove Tag and transmit the packet. • The VLAN ID list does not include the VLAN ID of the packet, discard the packet.
Trunk	Add Native VLAN Tag.	<ul style="list-style-type: none"> • Receive the packet if the packet VLAN ID is included in the permit passing VLAN ID list. • Discard the packet if the packet VLAN ID is not included in the permit passing VLAN ID list. 	<ul style="list-style-type: none"> • VLAN ID = Native VLAN ID, permit passing from interface, remove Tag and transmit the packet. • VLAN ID ≠ Native VLAN ID, permit passing from interface, transmit the packet with Tag.



Note

- By default, the default VLAN on the A10E/A28E is VLAN 1.
- By default, the Access VLAN of the Access interface is VLAN 1, and the Native VLAN of the Trunk interface is VLAN 1.
- By default, VLAN 1 is in the list permitted by all interfaces. Use the **switchport access egress-allowed vlan** { { **all** | *vlan-list* } [**confirm**] | { **add** | **remove** } *vlan-list* } command to modify the VLAN list allowed to pass by the Access interface. Use the **switchport trunk allowed vlan** { { **all** | *vlan-list* } [**confirm**] | { **add** | **remove** } *vlan-list* } command to modify the VLAN list allowed to pass by the Trunk interface.

2.2.2 Preparing for configurations

Scenario

Main function of VLAN is to divide logic network segments. There are 2 typical application modes:

- One kind is in small size LAN, one device is carved up to several VLAN, the hosts that connect to the device are carved up by VLAN. So hosts in the same VLAN can communicate, but hosts between different VLAN cannot communicate. For example, the financial department needs to divide from other departments and they cannot access each other. Generally, the interface to connect host is in Access mode.
- The other kind is in bigger LAN or enterprise network, multiple devices connected to multiple hosts and the devices are concatenated, data packet takes VLAN Tag for forwarding. Identical VLAN interface of multiple devices can communicate, but hosts between different VLAN cannot communicate. This mode is used in enterprise that has many employees and needs a large number of hosts, in the same department but different position, the hosts in one department can access one another, so customer has to divide VLANs on multiple devices. Layer 3 devices like router is required if users want to communicate among different VLAN. The concatenated interfaces among devices are set in Trunk mode.

When configuring IP address for VLAN, you can associate a Layer 3 interface for it. Each Layer 3 interface is corresponding to one IP address and one VLAN.

Prerequisite

N/A

2.2.3 Default configurations of VLAN

The default configuration of VLAN is as below.

Function	Default value
Create VLAN	VLAN 1
Active status of static VLAN	suspend
Interface mode	Access
Access VLAN of the Access interface	VLAN 1

Function	Default value
Native VLAN of the Trunk interface	VLAN 1
Allowed VLAN in Trunk mode	All VLANs
Allowed Untag VLAN in Trunk mode	VLAN 1

2.2.4 Configuring VLAN attributes

Configure VLAN attributes as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# create vlan <i>vlan-list</i> { active suspend }	Create VLAN. The command can also be used to create VLAN in batches.
3	Alpha-A28E(config)# vlan <i>vlan-id</i>	Enter VLAN configuration mode.
4	Alpha-A28E(config-vlan)# name <i>vlan-name</i>	(Optional) configure VLAN name.
5	Alpha-A28E(config-vlan)# state { active suspend }	Configure VLAN in active or suspend status.



Note

- The VLAN created by the command **vlan** *vlan-id* is in suspend status, you need to use the command of **state active** to activate VLAN if they want to make it effective in system.
- By default, there is VLAN 1, the default VLAN (VLAN 1), all interfaces in Access mode belong to the default VLAN. VLAN 1 cannot be created and deleted.
- By default, the default VLAN (VLAN 1) is called Default; cluster VLAN Other VLAN is named as "VLAN + 4-digit VLAN ID", for example, VLAN 10 is named VLAN 0010 by default, and VLAN4094 is named as "VLAN 4094" by default.
- All configurations of VLAN are not effective until the VLAN is activated. When VLAN status is Suspend, you can configure the VLAN, such as delete/add interface, set VLAN name, etc. The system will keep the configurations, once the VLAN is activated, the configurations will take effect in the system.

2.2.5 Configuring interface mode

Configure interface mode as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# switchport mode { access trunk }	Set the interface to Access or Trunk mode.

2.2.6 Configuring VLAN on Access interface

Configure VLAN on the Access interface for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# switchport mode access Alpha-A28E(config-port)# switchport access vlan <i>vlan-id</i>	Configure interface in Access mode and add Access interface into VLAN.
4	Alpha-A28E(config-port)# switchport access egress-allowed vlan { { all <i>vlan-list</i> } [confirm] { add remove } <i>vlan-list</i> }	(Optional) configure Access interface permitted VLAN.

Note

- The interface allows Access VLAN packets to pass regardless of configuration for VLAN permitted by Access interface. The forwarded packets do not carry VLAN TAG.
- When setting Access VLAN, the system creates and activates VLAN automatically if you have not created and activated VLAN in advance.
- If you delete or suspend Access VLAN manually, system will set the interface Access VLAN as default VLAN by automation.
- If the configured Access VLAN is not default VLAN and there is no default VLAN in allowed VLAN list of Access interface, the interface does not permit default VLAN packets to pass.
- Allowed VLAN list of Access interface is only effective to static VLAN, and ineffective to cluster VLAN, GVRP dynamic VLAN, etc.

2.2.7 Configuring VLAN on the Trunk interface

Configure VLAN on Trunk interface for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# switchport mode trunk	Configure interface in Trunk mode.
4	Alpha-A28E(config-port)# switchport trunk native vlan <i>vlan-id</i>	Configure interface Native VLAN.
5	Alpha-A28E(config-port)# switchport trunk allowed vlan { { all <i>vlan-</i> <i>list</i> } [confirm] { add remove } <i>vlan-list</i> }	(Optional) configure VLANs allowed to pass by the Trunk interface.
6	Alpha-A28E(config-port)# switchport trunk untagged vlan { { all <i>vlan-</i> <i>list</i> } [confirm] { add remove } <i>vlan-list</i> }	(Optional) configure Untag VLANs allowed to pass by the Trunk interface.



Note

- The interface permits Native VLAN packets passing regardless of configuration on Trunk interface permitted VLAN list and Untagged VLAN list, the forwarded packets do not take with VLAN TAG.
- System will create and activate the VLAN if there is no VLAN was created and activated in advance when setting Native VLAN.
- System set the interface Trunk Native VLAN as default VLAN if user has deleted or blocked Native VLAN by manual.
- Interface permits in and out of Trunk Allowed VLAN packet. If the VLAN is Trunk Untagged VLAN, the packets remove VLAN TAG at egress interface, otherwise, do not modify the packets.
- If the configured Native VLAN is not default VLAN, and there is no default VLAN in Trunk interface permitted VLAN list, the interface will not permit default VLAN packets to pass.
- When setting Trunk Untagged VLAN list, system automatically adds all Untagged VLAN into Trunk permitted VLAN.
- Trunk permitted VLAN list and Trunk Untagged VLAN list are only effective to static VLAN, and ineffective for cluster VLAN, GVRP dynamic VLAN, etc.

2.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show vlan [<i>vlan-</i> <i>list</i> static dynamic]	Show VLAN configuration.
2	Alpha-A28E# show interface port [<i>port-id</i>] switchport	Show interface VLAN configuration.

2.3 QinQ

2.3.1 Introduction

QinQ (also known as Stacked VLAN or Double VLAN) technique is an extension for 802.1Q defined in IEEE 802.1ad standard.

Basic QinQ is a simple Layer 2 VPN tunnel technique, which encapsulate outer VLAN Tag for user private network packet at the carrier access end, then the packet takes double VLAN Tag to transmit through backbone network (public network) of carrier. In public network, packet just be transmitted in accordance with outer VLAN Tag (namely the public network VLAN Tag), the user private network VALN Tag is transmitted as data in packet.

This technique can save public network VLAN ID resource. You can mark out private network VLAN ID to avoid conflict with public network VLAN ID.

Basic QinQ

Figure 2-3 shows typical networking with basic QinQ, with the A10E/A28E as the Provider Edge (PE).

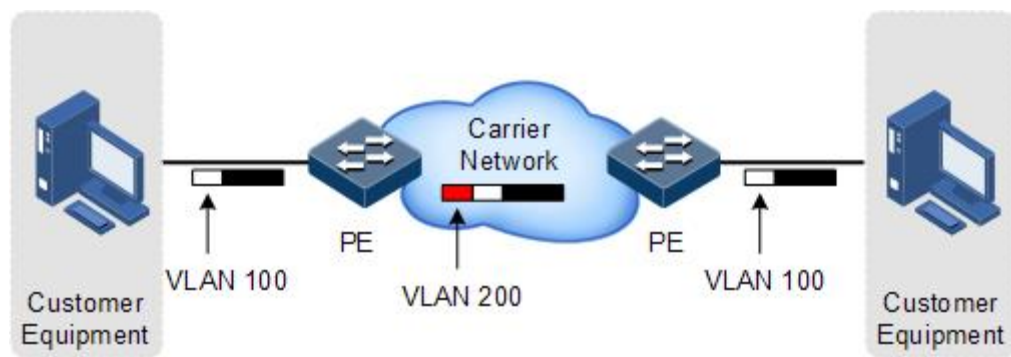


Figure 2-3 Typical networking with basic QinQ

The packet transmitted to the switch from user device, and the VLAN ID of packet tag is 100. The packet will be printed outer tag with VLAN 200 when passing through PE device user side interface and then enter PE network.

The VLAN 200 packet is transmitted to PE device on the other end by the carrier, and then the other Switch will strip the outer tag VLAN 200 and send it to the user device. So the packet returns to VLAN 100 tag.

Selective QinQ

Selective QinQ is an enhancement of basic QinQ. This technique is realized by combination of interface and VLAN. Selective QinQ can implement all functions of basic QinQ, and can even perform different actions on different VLAN Tags received by one interface and add different outer VLAN IDs for different inner VLAN IDs. By configuring mapping rules for inner and outer Tag, you can encapsulate different outer Tag for different inner Tag packet.

Selective QinQ makes carrier network structure more flexible. You can classify different terminal users at access device interface by VLAN Tag and then, encapsulate different outer Tag for different class users. On the Internet, you can configure QoS policy according to outer

Tag and configure data transmission priority flexibly so as to make users in different class receive the corresponding services.

2.3.2 Preparing for configurations

Scenario

With application of basic QinQ, you can add outer VLAN Tag to plan Private VLAN ID freely so as to make the user device data at both ends of carrier network take transparent transmission without conflicting with VLAN ID in service provider network.

Prerequisite

- Connect the interface and configure interface physical parameters to make the physical status Up.
- Create VLANs.

2.3.3 Default configurations of QinQ

The default configuration of QinQ is as below.

Function	Default value
Outer Tag TPID	0x8100
Basic QinQ status	Disable

2.3.4 Configuring basic QinQ

Configure basic QinQ on the ingress interface as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mls double-tagging tpid tpid	(Optional) configure TPID.
3	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
4	Alpha-A28E(config-port)# switchport qinq dot1q-tunnel	Enable basic QinQ on the interface.

2.3.5 Configuring selective QinQ

Configure selective QinQ on the ingress interface as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mls double-tagging tpid tpid	(Optional) configure TPID.
3	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
4	Alpha-A28E(config-port)# switchport vlan-mapping vlan-list add-outer vlan-id [cos cos-value]	Configure selective QinQ rules on the interface.

2.3.6 Configuring the egress interface to Trunk mode

Configure basic QinQ or selective QinQ on the network side interface as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# switchport mode trunk	Configure interface trunk mode, allowing double Tag packet to pass.

2.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show switchport qinq	Show configurations of basic QinQ.
2	Alpha-A28E# show interface interface-type interface-number vlan-mapping add-outer	Show configurations of selective QinQ.

2.3.8 Maintenance

Use the following commands to check configuration results.

Item	Description
Alpha-A28E(config)# clear double-tagging-vlan statistics outer { vlan-id any } inner { vlan-id any }	Clear statistics of double VLAN Tag packets.

2.3.9 Example for configuring basic QinQ

Networking requirements

As shown in Figure 2-4, Switch A and Switch B are connected to VLAN 100 and VLAN 200 respectively. Department C and department E need to communicate through the carrier network. Department D and Department F need to communicate, too. Thus, you need to set the outer Tag to VLAN 1000. Set Port 2 and Port 3 to dot1q-tunnel mode on Switch A and Switch B, and connect these two interfaces two different VLANs. Port 1 is the uplink interface connected to the ISP, and it is set to the Trunk mode to allow double Tag packets to pass. The carrier TPID is 9100.

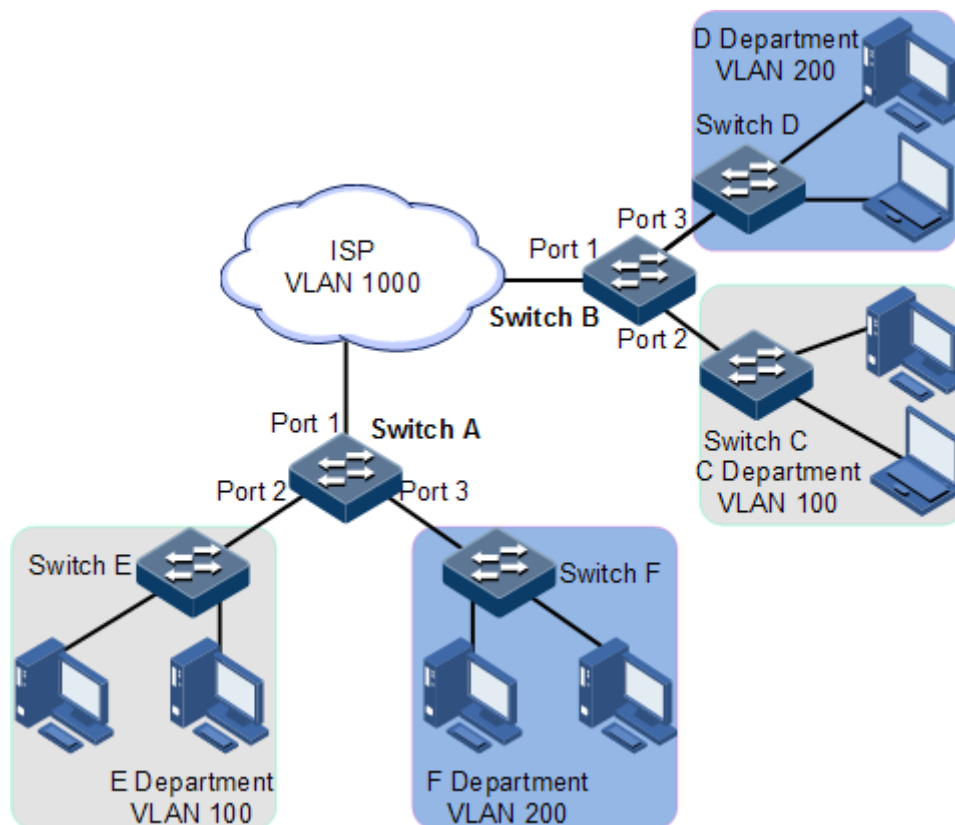


Figure 2-4 Basic QinQ networking application

Configuration steps

Step 1 Create VLAN 100, VLAN 200, and VLAN 1000 and activate them. TPID is 9100.

Configure Switch A.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#mls double-tagging tpid 9100
SwitchA(config)#create vlan 100,200,1000 active
```

Configure Switch B.

```
Alpha-A28E#hostname SwitchB
SwitchB#config
SwitchB(config)#mls double-tagging tpid 9100
SwitchB(config)#create vlan 100,200,1000 active
```

Step 2 Set Port 2 and Port 3 to dot1q mode.

Configure Switch A.

```
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk native vlan 1000
SwitchA(config-port)#switchport qinq dot1q-tunnel
SwitchA(config-port)#exit
SwitchA(config)#interface port 3
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk native vlan 1000
SwitchA(config-port)#switchport qinq dot1q-tunnel
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk native vlan 1000
SwitchB(config-port)#switchport qinq dot1q-tunnel
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk native vlan 1000
SwitchB(config-port)#switchport qinq dot1q-tunnel
SwitchB(config-port)#exit
```

Step 3 Set Port 1 to allow double Tag packets to pass.

Configure Switch A.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 1000 confirm
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk allowed vlan 1000 confirm
```

Checking result

Use the **show switchport qinq** command to view QinQ configurations.

Take Switch A for example.

```
SwitchA#show switchport qinq
Outer TPID: 0x9100
Interface      Qinq Status
-----
1              --
2              Dot1q-tunnel
3              Dot1q-tunnel
...
```

2.3.10 Example for configuring selective QinQ

Networking requirements

As shown in Figure 2-5, the carrier network contains common PC Internet service and IP phone service. PC Internet service is assigned to VLAN 1000, and IP phone service is assigned to VLAN 2000.

Configure Switch A and Switch B as below to make client and server communicate through carrier network:

- Add outer Tag VLAN 1000 to the VLANs 100–150 assigned to PC Internet service.
- Add outer Tag 2000 for VLANs 300–400 for IP phone service.
- The carrier TPID is 9100.

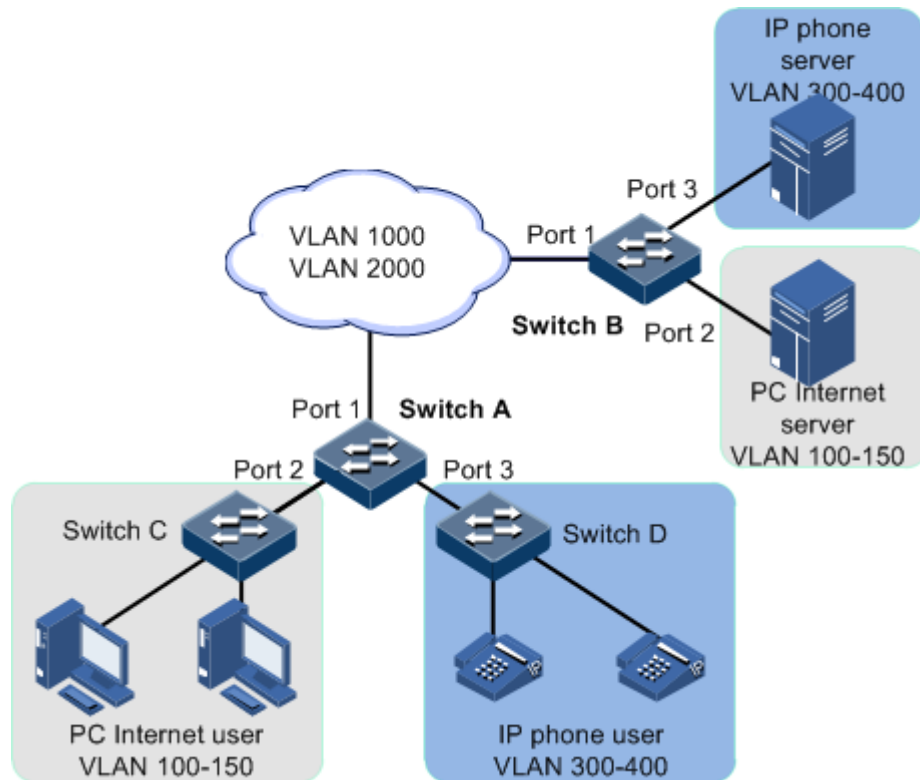


Figure 2-5 Selective QinQ networking application

Configuration steps

Step 1 Create and activate VLAN 100, VLAN 200, and VLAN 1000. The TPID is 9100.

Configure Switch A.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#mls double-tagging tpid 9100
SwitchA(config)#create vlan 100-150,300-400,1000,2000 active
```

Configure Switch B.

```
Alpha-A28E#hostname SwitchB
SwitchB#config
SwitchB(config)#mls double-tagging tpid 9100
SwitchB(config)#create vlan 100-150,300-400,1000,2000 active
```

Step 2 Set Port 2 and Port 3 to dot1q mode.

Configure Switch A.


```
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport vlan-mapping 100-150 add-outer 1000
SwitchA(config-port)#switchport trunk untagged vlan 1000,2000 confirm
SwitchA(config-port)#exit
SwitchA(config)#interface port 3
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport vlan-mapping 300-400 add-outer 2000
SwitchA(config-port)#switchport trunk untagged vlan 1000,2000 confirm
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport vlan-mapping cvlan 100-150 add-outer 1000
SwitchB(config-port)#switchport trunk untagged vlan 1000,2000 confirm
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport vlan-mapping cvlan 300-400 add-outer 2000
SwitchB(config-port)#switchport trunk untagged vlan 1000,2000 confirm
SwitchB(config-port)#exit
```

Step 3 Set Port 1 to allow double Tag packets to pass.

Configure Switch A.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 1000,2000 confirm
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk allowed vlan 1000,2000 confirm
```

Checking result

Use the **show interface port *port-id* vlan-mapping add-outer** command to view QinQ configuration.

Take Switch A for example.

```
SwitchA#show interface port 2 vlan-mapping add-outer
Based inner VLAN QinQ mapping rule:
Port Original Inner VLAN List      Add-outer VLAN Hw Status  Hw-ID
-----
2          100-150                    1000           Enable    1
SwitchA#show interface port 3 vlan-mapping add-outer
Based inner VLAN QinQ mapping rule:
Port Original Inner VLAN List      Add-outer VLAN Hw Status  Hw-ID
-----
3          300-400                    2000           Enable    2
```

2.4 VLAN mapping

2.4.1 Introduction

VLAN Mapping is mainly used to replace the private VLAN Tag of Ethernet packets with ISP's VLAN Tag, making packets transmitted according to ISP's VLAN forwarding rules. When packets are sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Therefore packets are correctly sent to the destination.

Figure 2-6 shows the principle of VLAN mapping.

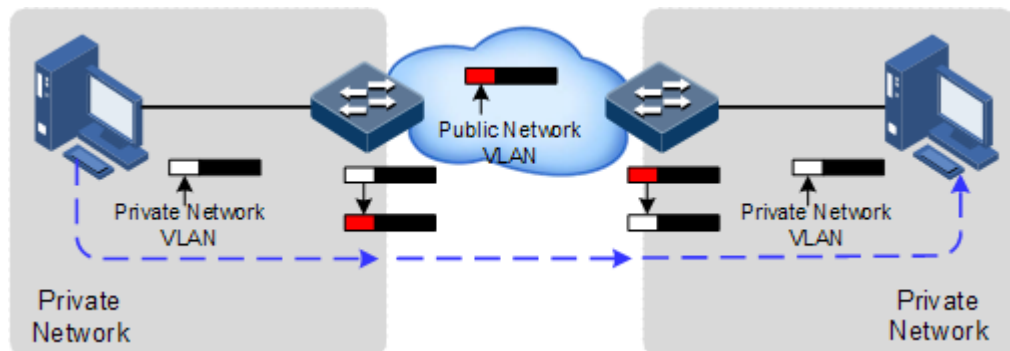


Figure 2-6 Networking with VLAN mapping based on single Tag

After receiving a VLAN Tag contained in a user private network packet, the A10E/A28E matches the packet according to configured VLAN mapping rules. If it matches successfully, it maps the packet according to configured VLAN mapping rules. The A10E/A28E supports the following mapping modes:

- 1:1 VLAN mapping: the A10E/A28E replaces the VLAN Tag carried by a packet from a specified VLAN to the new VLAN Tag.
- N:1 VLAN mapping: the A10E/A28E replaces the different VLAN Tags carried by packets from two or more VLANs with the same VLAN Tag.

Different from QinQ, VLAN mapping does not encapsulate packets with multiple layers of VLAN Tags, but needs to modify VLAN Tag so that packets are transmitted according to the carrier's VLAN forwarding rules.

2.4.2 Preparing for configurations

Scenario

Different from QinQ, VLAN mapping is to change the VLAN Tag without encapsulating multilayer VLAN Tag so that packets are transmitted according to the carrier's VLAN mapping rules. VLAN mapping does not increase the frame length of the original packet. It can be used in the following scenarios:

- A user service needs to be mapped to a carrier's VLAN ID.
- Multiple user services need to be mapped to a carrier's VLAN ID.

Prerequisite

Before configuring VLAN mapping,

- Connect the interface and configure its physical parameters to make it Up.
- Create a VLAN.

2.4.3 Configuring 1:1 VLAN mapping

Configure 1:1 VLAN mapping as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# switchport vlan-mapping [egress ingress] cvlan-list translate vlan-id	Configure interface-based 1:1 VLAN mapping rules in the ingress or egress direction.

2.4.4 Configuring N:1 VLAN mapping

Configure N:1 VLAN mapping as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# switchport vlan-mapping both n-to-1 cvlan-list translate svlan-id	Configure rules of Tag-based N:1 VLAN mapping rules.

Step	Configuration	Description
4	Alpha-A28E(config-port)# switchport vlan-mapping both n-to-1 cvlan-list translate dtag svlan-id cvlan-id	Configure rules of double-Tag-based N:1 VLAN mapping rules.
5	Alpha-A28E(config-port)# switchport vlan-mapping both untag translate dtag svlan-id cvlan-id	Configure selective QinQ and double Tag rules on the interface.

2.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show interface port [port-id] vlan-mapping { egress ingress } translate	Show configurations of 1:1 VLAN mapping.
2	Alpha-A28E# show interface port [port-id] vlan-mapping both translate	Show configurations of N:1 VLAN mapping on the interface.
3	Alpha-A28E# show interface port [port-id] vlan-mapping both untag	Show configurations of selective QinQ and double Tag rules on the interface.

2.4.6 Example for configuring VLAN mapping

Networking requirements

As shown in Figure 2-7, Port 2 and Port 3 of Switch A are connected to Department E of VLAN 100 and Department F of VLAN 200, Port 2 and Port 3 of Switch B are connected to Department C of VLAN 100 and Department D of VLAN 200. The ISP assigns VLAN 1000 to transmit packets of Department E and Department C, and VLAN 2008 to transmit packets of Department F and Department D.

Configure 1:1 VLAN mapping on the Switch A and Switch B to implement normal communication between PC or terminal users and servers.

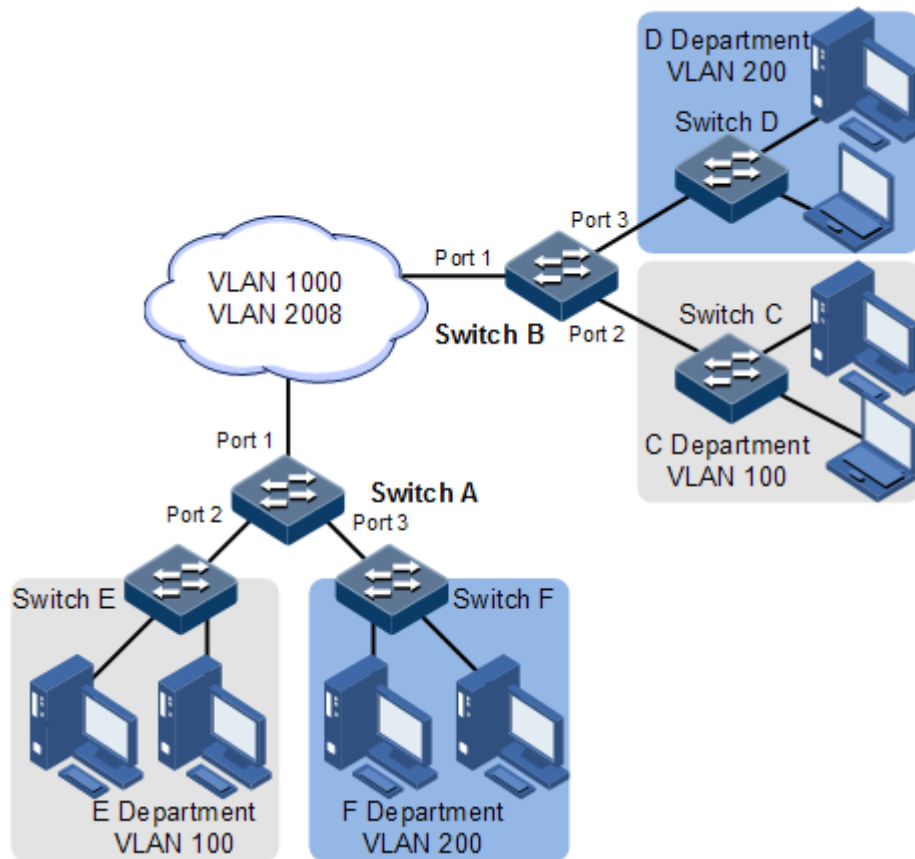


Figure 2-7 VLAN mapping application networking

Configuration steps

Configurations of Switch A and Switch B are the same. Take Switch A for example.

Step 1 Create VLANs and activate them.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100,200,1000,2008 active
SwitchA(config)#vlan-mapping enable
```

Step 2 Set Port 1 to Trunk mode, allowing packets of VLAN 1000 and VLAN 2008 to pass.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 1000,2008 confirm
SwitchA(config-port)#exit
```

Step 3 Set Port 2 to Trunk mode, allowing packets of VLAN 100 to pass. Enable VLAN mapping.

```
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 100 confirm
SwitchA(config-port)#switchport vlan-mapping ingress 100 translate 1000
SwitchA(config-port)#switchport vlan-mapping egress 1000 translate 100
SwitchA(config-port)#exit
```

Step 4 Set Port 3 to Trunk mode, allowing packets of VLAN 200 to pass. Enable VLAN mapping.

```
SwitchA(config)#interface port 3
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 200 confirm
SwitchA(config-port)#switchport vlan-mapping ingress 200 translate 2008
SwitchA(config-port)#switchport vlan-mapping egress 2008 translate 200
```

Checking result

Use the **show interface port *port-id* vlan-mapping { ingress | egress } translate** command to show configurations of 1:1 VLAN mapping.

```
SwitchA#show interface port 2 vlan-mapping ingress translate
Direction: Ingress
          Original   Original   Outer-tag New   Inner-tag New
Interface Inner VLANs Outer VLANs Mode   Outer-VID Mode   Inner-VID
HW-ID
-----
2          n/a       100       Translate 1000   --     --
```

2.5 Interface protection

2.5.1 Introduction

Layer 2 data needs to be isolated from different interfaces, so you can add these interfaces to different VLANs. Sometimes, Layer 2 data needs to be isolated from the interfaces in the same VLAN, so interface protection can be used to isolate these interfaces.

Through interface protection, you can enable the protection feature to interfaces needed to be controlled to achieve the Layer 2 data isolation and reach physical isolation effect among interfaces, which improve network security and provide flexible networking solution to customers.

The packets among interfaces in a protection group cannot communicate after configuring interface protection, but the communication between interfaces enabling interface protection and disabling interface protection will not be influenced.

2.5.2 Preparing for configurations

Scenario

To isolate Layer 2 data from the interfaces in the same VLAN, like physical isolation, you need to configure interface protection.

The interface protection function can realize mutual isolation of the interfaces in the same VLAN, enhance network security and provide flexible networking solutions for you.

Prerequisite

N/A

2.5.3 Default configurations of interface protection

The default configuration for interface protection is as below.

Function	Default value
Interface protection function status of each interface	Disable

2.5.4 Configuring interface protection

Configure interface protection for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# switchport protect	Enable interface protection.

2.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show switchport protect	Show interface protection configuration.

2.5.6 Example for configuring interface protection

Networking requirements

As shown in Figure 2-7, PC 1, PC 2, and PC 5 belong to VLAN 10, and PC 3 and PC 4 belong to VLAN 20. The interfaces connecting two devices are in Trunk mode, but do not allow VLAN 20 packets to pass. As a result, PC 3 and PC 4 fail to communicate with each other. Enable interface protection on the interfaces of PC 1 and PC 2 which are connected to Switch B. As a result, PC 1 and PC 2 fail to communicate with each other, but they can communicate with PC 5 respectively.

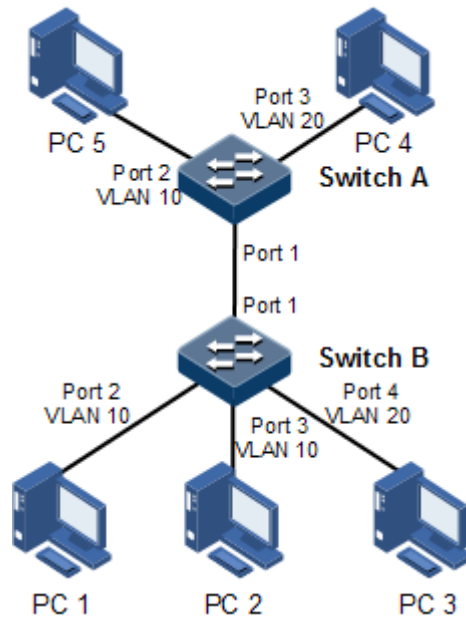


Figure 2-8 Interface protection application networking

Configuration steps

Step 1 Create VLAN 10 and VLAN 20 on both Switch A and Switch B, and activate them.

Configure Switch A.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 10,20 active
```

Configure Switch B.

```
Alpha-A28E#hostname SwitchB
SwitchB#config
SwitchB(config)#create vlan 10,20 active
```


- Step 2 Add Port 2 and Port 3 of Switch B to VLAN 10 in Access mode, add Port 4 to VLAN 20 in Access mode, and set Port 1 in Trunk mode to allow VLAN 10 packets to pass.

```
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 10
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 10
SwitchB(config-port)#exit
SwitchB(config)#interface port 4
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 20
SwitchB(config-port)#exit
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk allowed vlan 10 confirm
SwitchB(config-port)#exit
```

- Step 3 Add Port 2 of Switch A to VLAN 10 in Access mode, add Port 3 to VLAN 20 in Trunk mode, and set Port 1 in Trunk mode to allow VLAN 10 packets to pass.

```
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode access
SwitchA(config-port)#switchport access vlan 10
SwitchA(config-port)#exit
SwitchA(config)#interface port 3
SwitchA(config-port)#switchport mode access
SwitchA(config-port)#switchport access vlan 20
SwitchA(config-port)#exit
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 10 confirm
```

- Step 4 Enable interface protection on Port 2 and Port 3 on Switch B.

```
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport protect
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport protect
```

Checking results

Use the **show vlan** command to check whether VLAN configurations are correct.

Take Switch B for example.

```
SwitchB#show vlan
VLAN Name      State  Status  Port      Untag-Port  Priority  Create-Time
-----
1   Default      active static  1-10      1-10        --       0:0:7
10  VLAN0010     active static  1-3       2,3         --       0:1:1
20  VLAN0020     active static  4         4           --       0:1:1
```

Use the **show interface port *port-id* switchport** command to check whether interface VLAN is correctly configured.

Take Switch B for example.

```
SwitchB#show interface port 2 switchport
Port:2
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 10
Administrative Access Egress VLANs: 1
Operational Access Egress VLANs: 1,10
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: 1,10,20
Administrative Trunk Untagged VLANs: 1
Operational Trunk Untagged VLANs: 1
```

Use the **show switchport protect** command to check whether interface protection is correctly configured.

```
SwitchB#show switchport protect
Port      Protected State
-----
1         disable
2         enable
3         enable
...
```

Check whether PC 1 can ping PC 5, PC 2 can ping PC 5, and PC 3 can ping PC 4 successfully. Check whether the VLAN allowed to pass on the Trunk interface is correct.

- If PC 1 can ping PC 5 successfully, VLAN 10 communicates properly.
- If PC 2 can ping PC 5 successfully, VLAN 10 communicates properly.
- If PC 3 fails ping PC 4, VLAN 20 fails to communicate.

By pinging PC 2 through PC 1, check whether interface protection is correctly configured.

PC 1 fails to ping PC 3, so interface protection has taken effect.

2.6 Port mirroring

2.6.1 Introduction

Port mirroring refers to assigning some packets mirrored from the source interface to the destination interface, such as from the monitor port without affecting the normal packet forwarding. You can monitor sending and receiving status for packets on an interface through this function and analyze the relevant network conditions.

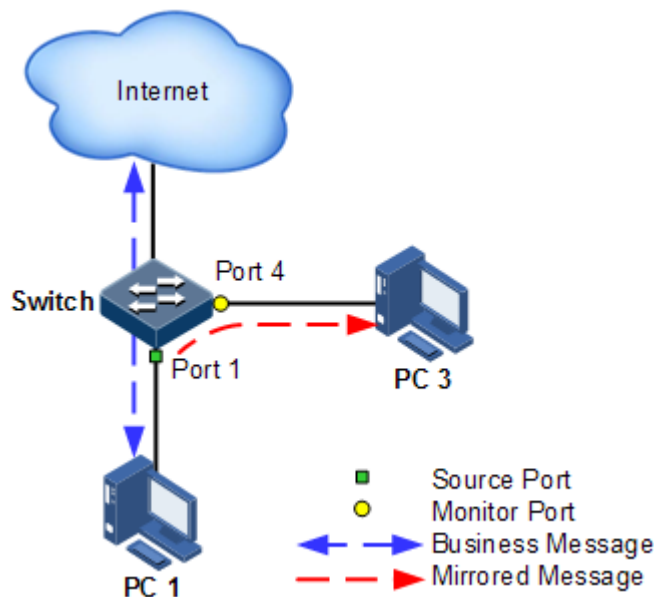


Figure 2-9 Port mirroring principle

The basic principle of port mirroring is shown in Figure 2-9. PC 1 connects outside network via the Port 1; PC 3 is the monitoring PC, connecting the external network through Port 4.

When monitoring packets from the PC 1, you need to assign Port 1 to connect to PC1 as the mirroring source port, enable port mirroring on the ingress port and assign Port 4 as monitor port to mirror packets to destination port.

When service packets from PC 1 enter the switch, the switch will forward and copy them to monitor port (Port 4). The monitoring device connected to mirror the monitoring interface can receive and analyze these mirrored packets.

The A10E/A28E supports data stream mirroring on the ingress port and egress port. The packets on ingress/egress mirroring port will be copied to the monitor port after the switch is enabled with port mirroring. The monitor port and mirroring port cannot be the same one.

2.6.2 Preparing for configurations

Scenario

Port mirroring is mainly used to monitor network data type and flow regularly for the network administrator.

Interface mirroring function is to copy the interface flow monitored to a monitor interface or CPU so as to obtain the ingress/egress interface failure or abnormal flow of data to analyze, discover the root cause and solve them timely.

Prerequisite

N/A

2.6.3 Default configurations of port mirroring

The default configuration of port mirroring is as below.

Function	Default value
Port mirroring status	Disable
Mirror source interface	N/A
Mirror monitoring interface	Port 1



Note

When you configure to mirror packets to the CPU, the monitor port receives no packets.

2.6.4 Configuring port mirroring on a local port



Caution

- There can be multiple source mirroring ports but only one monitor port.
- The ingress/egress mirroring port packet will be copied to the monitor port after port mirroring takes effect. The monitor port cannot be set to the mirroring port again.

Configure local port mirroring for the A10E/A28E as below.

Step	Configure	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mirror monitor-port <i>port-id</i>	Configure the packet mirror of port mirroring to CPU or specified monitor interface.
3	Alpha-A28E(config)# mirror source-port-list { both <i>port-list</i> egress <i>port-list</i> ingress <i>port-list</i> [egress <i>port-list</i>] }	Configure the mirror source interface of port mirroring and designate the mirror rule for port mirroring.
4	Alpha-A28E(config)# mirror enable	Enable port mirroring.

2.6.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show mirror	Show port mirroring configuration.

2.6.6 Example for configuring port mirroring

Networking requirements

As shown in Figure 2-10, the network administrator hopes to monitor on user network 1 through data monitor device, then to catch the fault or abnormal data flow for analyzing and discovering problem and then solve it.

The A10E/A28E is disabled with storm control and automatic packets sending. User network 1 accesses the A10E/A28E through Port 2, user network 2 accesses the A10E/A28E through Port 1, and data monitor device is connected to Port 3.

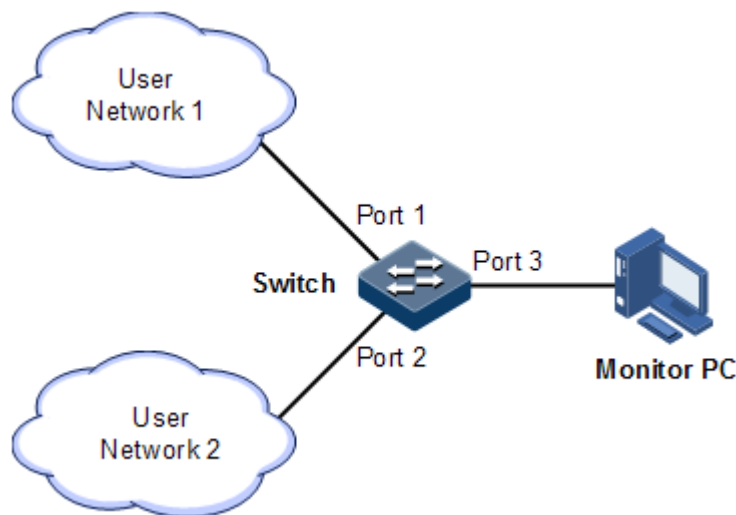


Figure 2-10 Port mirroring application networking

Configuration steps

Enable port mirroring on the switch.

```
Alpha-A28E#config  
Alpha-A28E(config)#mirror monitor-port 3  
Alpha-A28E(config)#mirror source-port-list both 1  
Alpha-A28E(config)#mirror enable
```

Checking results

Show interface mirror information by the command of **show mirror**.

```
Alpha-A28E#show mirror
Mirror: Enable
Monitor port: 3
Non-mirror port: Not block
-----the both mirror rule-----
Mirrored ports: 1
Divider: 0
MAC address: 0000.0000.0000
-----the both mirror rule-----
Mirrored ports: --
Divider: 0
MAC address: 0000.0000.0000
```

2.7 Layer 2 protocol transparent transmission

2.7.1 Introduction

Transparent transmission function is one of the main Ethernet device functions, usually the edge network devices of carrier take charge of Layer 2 protocol packet transparent transmission. Transparent transmission function is enabled at the interface that connects edge network devices of carrier and user network. The interface is in Access mode, connecting to Trunk interface on user device. The layer 2 protocol packet of user network enters from transparent transmission interface, encapsulated by edge network device (ingress end of packet) and then enter carrier network. The packet is transmitted through carrier network to reach edge device (egress end of packet) at the other end or carrier network. The edged device decapsulates outer layer 2 protocol packet and transparent transmits it to user network.

The transparent transmission function includes packet encapsulation and decapsulation function, the basic implementing principle as below.

- Packet encapsulation: at the packet ingress end, the A10E/A28E modifies destination MAC address from user network layer 2 protocol packets to special multicast MAC address (it is 010E.5E00.0003 by default). In carrier network, the modified packet is forwarded as data in user VLAN.
- Packet decapsulation: at the packet egress end, the A10E/A28E senses packet with special multicast MAC address (it is 010E.5E00.0003 by default) and revert the destination MAC address to DMAC of Layer 2 protocol packets, then send the packet to assigned user network.

Layer 2 protocol transparent transmission function can be operated at the same time with QinQ or operated independently. In practice application, after modifying protocol packet MAC address, need to add outer Tag for transmit through carrier network.

The A10E/A28E supports transparent transmission of BPDU packet, DOT1X packet, LACP packet, CDP packet, PVST packet, PAGP packet, STP packet, UDLD packet and VTP packet.

2.7.2 Preparing for configurations

Scenario

This function enables layer 2 protocol packets of one user network cross through carrier network to make one user network unified operating one Layer 2 protocol at different region. You can configure rate limiting on transparent transmission packets to prevent packet loss.

Prerequisite

Configure physical parameters for the interface to set it in Up status before configuring Layer 2 protocol transparent transmission function.

2.7.3 Default configurations of Layer 2 protocol transparent transmission

The default configuration of Layer 2 protocol transparent transmission is as below.

Function	Default value
Layer 2 protocol transparent transmission status	Disable
Egress interface and belonged VLAN of Layer 2 protocol packet	NULL
TAG CoS value of transparent transmission packet	5
Destination MAC address of transparent transmission packet	010E.5E00.0003
Discarding threshold and disabling threshold of transparent transmission packet	NULL

2.7.4 Configuring transparent transmission parameters

Configure transparent transmission parameter for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# relay destination-address <i>mac-address</i>	(Optional) configure destination MAC for transparent transmission packet. The default value is 010E.5E00.0003.
3	Alpha-A28E(config)# relay cos <i>cos-value</i>	(Optional) configure CoS value for transparent transmission packet.
4	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode or aggregation group configuration mode.
5	Alpha-A28E(config-port)# relay port <i>port-id</i>	Configure specified egress interface for transparent transmission packet.

Step	Configuration	Description
6	Alpha-A28E(config-port)# relay vlan <i>vlan-id</i>	Configure specified VLAN for transparent transmission packet. The specified VLAN configuration can transmit the packet according to specified VLAN, but not VLAN configuration of ingress interface.
7	Alpha-A28E(config-port)# relay { all cdp dot1x lacp pagp pvst stp udld vtp }	Configure transparent transmission message type on the interface.

2.7.5 Checking configuration

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show relay [port-list <i>port-list</i>]	Show configurations and status of transparent transmission.
2	Alpha-A28E# show relay statistics [port-list <i>port-list</i>]	Show statistics of transparent transmission packets.

2.7.6 Maintenance

Maintain Ethernet features by the following commands.

Commands	Description
Alpha-A28E(config)# clear relay statistics [port-list <i>port-list</i>]	Clear statistics of transparent transmission packets.
Alpha-A28E(config-port)# no relay shutdown	Enable the interface again.

2.7.7 Configuring Layer 2 protocol transparent transmission

Networking requirements

As shown below, Switch A and Switch B connect to two user networks VLAN 100 and VLAN 200 respectively. You need to configure Layer 2 protocol transparent transmission function on Switch A and Switch B in order to make the same user network in different regions run STP entirely.

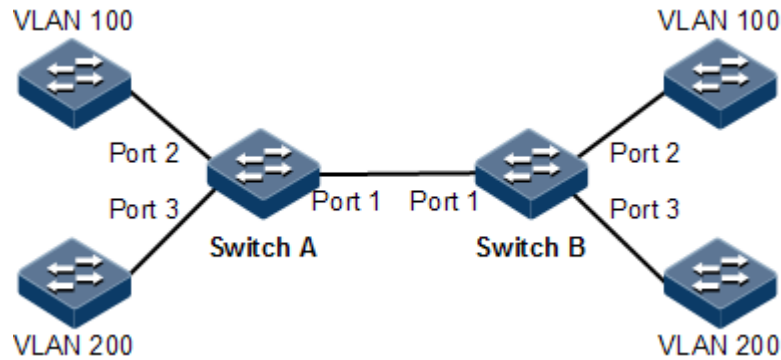


Figure 2-11 Layer 2 protocol transparent transmission application networking

Configuration steps

- Step 1 Create VLAN 100, 200 and activate them.

Configure Switch A.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100,200 active
```

Configure Switch B.

```
Alpha-A28E#hostname SwitchB
SwitchA#config
SwitchA(config)#create vlan 100,200 active
```

- Step 2 Set the switching mode of Port 2 to Access mode, set the Access VLAN to 100, and enable STP transparent transmission.

Configure Switch A.

```
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode access
SwitchA(config-port)#switchport access vlan 100
SwitchA(config-port)#relay stp
SwitchA(config-port)#relay port 1
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode access
```

```
SwitchB(config-port)#switchport access vlan 100
SwitchB(config-port)#relay stp
SwitchB(config-port)#relay port 1
SwitchB(config-port)#exit
```

- Step 3 Set the switching mode of Port 3 to Access mode, set the Access VLAN to 200, and enable STP transparent transmission.

Configure Switch A.

```
SwitchA(config)#interface port 3
SwitchA(config-port)#switchport mode access
SwitchA(config-port)#switchport access vlan 200
SwitchA(config-port)#relay stp
SwitchA(config-port)#relay port 1
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 200
SwitchB(config-port)#relay stp
SwitchB(config-port)#relay port 1
SwitchB(config-port)#exit
```

- Step 4 Set Port 1 to Trunk mode.

Configure Switch A.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
```

Checking result

Use the **show relay** command to check whether Layer 2 protocol transparent transmission is correctly configured.

Take Switch A for example.

```

SwitchA#show relay port-list 1-3
COS for Encapsulated Packets: 5
Destination MAC Address for Encapsulated Packets: 010E.5E00.0003
Port    vlan  Egress-Port  Protocol    Drop-Threshold  Shutdown-Threshold
-----
1(up)   --   --              stp         --              --
        dot1x        --              --
        lacp         --              --
        cdp         --              --
        vtp         --              --
        pvst        --
        udld        ---              ---
        pagp        ---
2(up)   --   1              stp(enable) --              --
        dot1x        --              --
        lacp         --              --
        cdp         --              --
        vtp         --              --
        pvst        --
        udld        ---              ---
        pagp        ---
3(up)   --   1              stp(enable) --              --
        dot1x        --              --
        lacp         --              --
        cdp         --              --
        vtp         --              --
        pvst        --

```

3 IP services

This chapter introduces basic principle and configuration of routing features, and provides the related configuration applications, including the following chapters:

- ARP
- Layer 3 interface
- Default gateway
- DHCP Client
- DHCP Relay
- DHCP Snooping
- DHCP options

3.1 ARP

3.1.1 Introduction

In TCP/IP network environment, each host is assigned with a 32-bit IP address that is a logical address used to identify host between networks. To transmit packet in physical link, you must know the physical address of destination host, which requires mapping IP address to physical address. In Ethernet environment, physical address is 48-bit MAC address. Users have to transfer the 32-bit destination host IP address to 48-bit Ethernet address for transmitting packet to destination host correctly. Then Address Resolution Protocol (ARP) is applied to analyze IP address to MAC address and set mapping relationship between IP address and MAC address.

ARP address mapping table includes the following two types:

- Static entry: bind IP address and MAC address to avoid ARP dynamic learning cheating.
 - Static ARP address entry needs to be added/deleted manually.
 - No aging to static ARP address.
- Dynamic entry: MAC address automatically learned through ARP.
 - This dynamic table entry is automatically generated by switch. You can adjust partial parameters of it manually.
 - The dynamic ARP address entry will age at the aging time if no use.

The A10E/A28E supports the following two ARP address mapping entry dynamic learning modes:

- Learn-all: in this mode, the A10E/A28E learns both ARP request packets and response packets. When device A sends its ARP request, it writes mapping between its IP address and physical address in ARP request packets. When device B receives ARP request packets from device A, it learns the mapping in its address table. In this way, device B will no longer send ARP request when sending packets to device A.
- Learn-reply-only mode: in this mode, the A10E/A28E learns ARP response packets only. For ARP request packets from other devices, it responds with ARP response packets only rather than learning ARP address mapping entry. In this way, network load is heavier but some network attacks based on ARP request packets can be prevented.

3.1.2 Preparing for configurations

Scenario

The mapping relation of IP address and MAC address is stored in ARP address mapping table.

Generally, ARP address mapping table is dynamic maintained by the A10E/A28E. The A10E/A28E searches the mapping relation between IP address and MAC address automatically according to ARP protocol. Users just need to configure the A10E/A28E manually for preventing ARP dynamic learning from cheating and adding static ARP address mapping table entry.

Prerequisite

N/A

3.1.3 Default configurations of ARP

The default configuration of ARP is as below.

Function	Default value
Static ARP table entry	N/A
Dynamic ARP entry learning mode	Learn-reply-only

3.1.4 Configuring static ARP table entries



Caution

- The IP address in static ARP table entry must belong to the IP network segment of switch Layer 3 interface.
- The static ARP table entry needs to be added and deleted manually.

Configure static ARP table entries for the A10E/A28E as below.

Step	Configuration	Description
1	A1pha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# arp <i>ip-address mac-address</i>	Configure static ARP table entry.

3.1.5 Configuring aging time of dynamic ARP entries

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# arp aging-time <i>period</i>	(Optional) configure dynamic ARP entry learning mode. The value 0 indicates no aging.

3.1.6 Configuring dynamic ARP entry learning mode

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# arp mode { learn-all learn-reply-only }	(Optional) configure dynamic ARP entry learning mode.

3.1.7 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show arp	Show information about ARP address table.
2	Alpha-A28E# show arp <i>ip-address</i>	Show ARP table information related to specified IP address.
3	Alpha-A28E# show arp ip <i>if-number</i>	Show ARP table information related to Layer 3 interface.
4	Alpha-A28E# show arp static	Show ARP statistics.

3.1.8 Maintenance

Maintain the A10E/A28E as below.

Command	Description
Alpha-A28E(config)# clear arp	Clear all entries in ARP address mapping table.

3.1.9 Configuring ARP

Networking requirements

As shown in Figure 3-1, the A10E/A28E connects to host, connects to the upstream router by Port 1. IP address of Router is 192.168.1.10/24, subnet mask is 255.255.255.0. MAC address is 0050-8d4b-fd1e.

To improve communication security between Device and Router, you need to configure related static ARP table entry on the A10E/A28E.

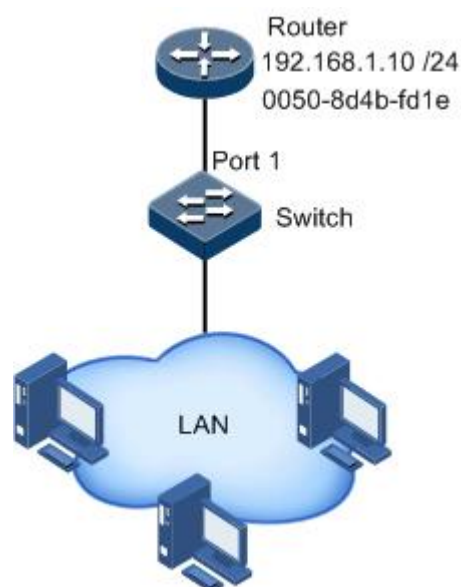


Figure 3-1 Configuring ARP networking application

Configuration steps

Step 1 Create an ARP static entry.

```
Alpha-A28E#config  
Alpha-A28E(config)#arp 192.168.1.10 0050.8d4b.fd1e
```

Checking results

Use the **show arp** command to check whether all the table entry information in ARP address mapping table is correct.

```
Alpha-A28E#show arp
ARP table aging-time: 1200 seconds(default: 1200s)
ARP mode: Learn reply only
Ip Address      Mac Address      Type   Interface ip
-----
192.168.1.10    0050.8d4b.fd1e   static --
192.168.100.1   000F.E212.5CA0   dynamic 1

Total: 2
Static: 1
Dynamic: 1
```

3.2 Layer 3 interface

3.2.1 Introduction

The Layer 3 interface refers to IP interface, and it is the virtual interface based on VLAN. Configuring Layer 3 interface is generally used for device network management or routing link connection of multiple devices. Associating a Layer 3 interface to VLAN requires configuring IP address; each Layer 3 interface will correspond to an IP address and associate with at least one VLAN.

If only one IP address is configured on Layer 3 interface of the A10E/A28E, only part of hosts can communicate with external networks through the switch. To enable all hosts to communicate with external networks, configure the secondary IP address of the interface. To enable hosts in two network segments to interconnect with each other, set the switch as gateway on all hosts.

3.2.2 Preparing for configurations

Scenario

You can connect a Layer 3 interface for VLAN when configuring IP address for it. Each Layer 3 interface will correspond to an IP address and connect a VLAN.

Prerequisite

Configure VLAN associated with interface and activate it before configuring Layer 3 interface.

3.2.3 Configuring the Layer 3 interface

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# interface ip <i>if-number</i>	Enter Layer 3 interface configuration mode.
3	Alpha-A28E(config- ip)# description <i>string</i>	Configure description of the Layer 3 interface.
4	Alpha-A28E(config-ip)# ip address <i>ip-address</i> [<i>ip-mask</i>] [<i>vlan-list</i>]	Configure the IP address of the Layer 3 interface, and associate with VLAN.
5	Alpha-A28E(config-ip)# ip vlan <i>vlan-list</i>	(Optional) configure the mapping between the Layer 3 interface and VLAN.



- Configure the VLAN associated with the Layer 3 interface, and the VLAN must be activated. Suspended VLAN can be activated through the **state { active | suspend }** command, and then configured. When you configure the mapping between a Layer 3 interface and a VLAN which does not exist or is deactivated, the configuration can be successful but does not take effect.
- Up to 15 IP interfaces can be configured, and they range from 0 to 14.

3.2.4 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show interface ip	Show IP address configuration of the Layer 3 interface.
2	Alpha-A28E# show interface ip description	Show mapping between Layer 3 interface and VLAN.
3	Alpha-A28E# show interface ip statistics	Show management VLAN configurations.

3.2.5 Example for configuring Layer 3 interface to interconnect with host

Networking requirements

As shown in Figure 3-2, configure the Layer 3 interface to the switch so that the host and the A10E/A28E can Ping each other.

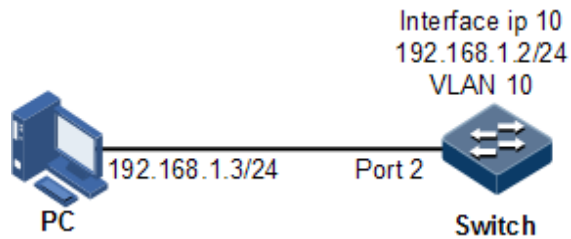


Figure 3-2 Layer 3 interface configuration networking

Configuration steps

Step 1 Create a VLAN and add the interface into VLAN.

```
Alpha-A28E#config
Alpha-A28E(config)#create vlan 10 active
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#switchport access vlan 10
```

Step 2 Configure Layer 3 interface on the A10E/A28E, and configure the IP address, and associate the IP address with the VLAN.

```
Alpha-A28E(config)#interface ip 10
Alpha-A28E(config-ip)#ip address 192.168.1.2 255.255.255.0 10
```

Checking results

Check whether the binding relation of VLAN and physical interface is correct by the command of **show vlan**:

```
Alpha-A28E#show vlan 10
VLAN Name      State  Status  Port      Untag-Port  Priority  Create-Time
-----
10  VLAN0010  active  static  2          2           --       1:16:49
```

Check whether the Layer 3 interface configuration is correct and whether the mapping between the Layer 3 interface and VLAN is correct by the command of **show interface ip**.

```
Alpha-A28E#show interface ip
Index  Ip Address      NetMask      Vid      Status  Mtu
-----
0      192.168.27.63  255.255.255.0  1        active  1500
10     192.168.1.2    255.255.255.0  10       active  1500
```

Check whether the A10E/A28E and PC can ping each other by the command of **ping**.

```
Alpha-A28E#ping 192.168.1.3
Type CTRL+C to abort
Sending 5, 8-byte ICMP Echos to 192.168.1.3, timeout is 3 seconds:
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms

---- PING Statistics----
5 packets transmitted, 5 packets received,
Success rate is 100 percent(5/5),
round-trip (ms)  min/avg/max = 0/0/0.
```

3.3 Default gateway

3.3.1 Introduction

When the packet to be forwarded is not configured with a route, you can configure the default gateway to enable a device to send the packet to the default gateway. The IP address of the default gateway should be in the same network segment with the local IP address of the device.

3.3.2 Preparing for configurations

Scenario

When the packet to be forwarded is not configured with a route, you can configure the default gateway to enable a device to send the packet to the default gateway.

Prerequisite

Configure the IP address of the switch in advance; otherwise, configuring the default gateway will fail.

3.3.3 Configuring the default gateway



Note

The IP address of the default gateway should be in the same network segment of any local IP interface.

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip default-gateway <i>ip-address</i>	Configure the IP address of the default gateway.

3.3.4 Configuring static route

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip forwarding	Enable software IP forwarding on the A10E/A28E.
3	Alpha-A28E(config)# ip route <i>ip-address ip-mask next-hop-ip-address</i>	Create a static route.

3.3.5 Checking configurations

Use the following command to check configuration result.

No.	Item	Description
1	Alpha-A28E# show ip route	Show routing table information.

3.4 DHCP Client

3.4.1 Introduction

Dynamic Host Configuration Protocol (DHCP) refers to assign IP address configuration information dynamically for users in TCP/IP network. It is based on BOOTP (Bootstrap Protocol) protocol, and automatically adds the specified available network address, network address re-use, and other extended configuration options over BOOTP protocol.

With enlargement of network scale and development of network complexity, quantity of PC in network usually exceeds available distributed IP address amount. Meanwhile, the widely use of notebooks and wireless networks lead to frequent change of PC positions and also the related IP address must update frequently. As a result, network configuration becomes more and more complex. DHCP is developed to solve these problems.

DHCP adopts client/server communication mode. The client applies configuration to the server (including IP address, Subnet mask, default gateway) and server replies IP address for client and other related configuration information to realize dynamic configuration of IP address, etc.

Typical application of DHCP usually includes a set of DHCP server and several clients (for example PC or Notebook), as shown below.

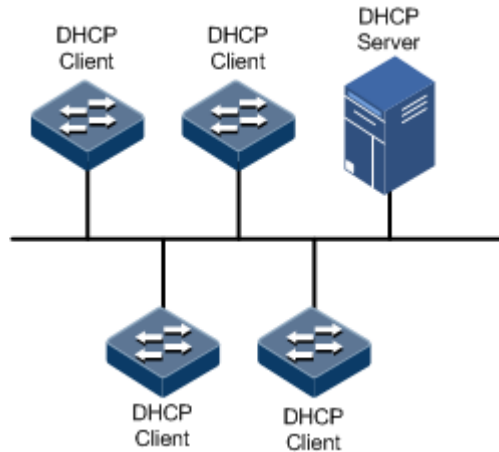


Figure 3-3 DHCP typical application networking

DHCP technology ensures the rational allocation, avoid the waste and improve the utilization rate of IP addresses in the entire network.

The format of DHCP packets is as shown below. DHCP packets are encapsulated in UDP data packets.

0	7	15	23	31
OP	Hardware type		Hardware length	Hops
Transaction ID				
Seconds		Flags		
Client IP address				
Your(client) IP address				
Server IP address				
Relay agent IP address				
Client hardware address				
Server host name				
File				
Options				

Figure 3-4 Structure of DHCP packets

Meaning of different fields in DHCP packets is shown below.

Table 3-1 Fields definition of DHCP packets

Field	Length	Description
OP	1	Packet type <ul style="list-style-type: none"> • Value at 1: it is request packets. • Value at 2: it is reply packets.
Hardware type	1	Hardware address type of DHCP client.
Hardware length	1	Hardware address size of DHCP client.

Field	Length	Description
Hops	1	Number of DHCP hops passed by the DHCP packet. It increases by 1 every time when DHCP request packet passes a DHCP hop.
Transaction ID	4	Client chooses number at random when starts a request, used to mark process of address request.
Seconds	2	DHCP client passed time after starting DHCP request. It is unused now, fixed as 0.
Flags	2	Bit 1 is broadcast reply flag, used to mark DHCP server reply packet is transmitted in unicast or broadcast mode. <ul style="list-style-type: none"> • 0: unicast • 1: broadcast Other bits are reserved.
Client IP address	4	DHCP client IP address, only be filled when client is bound, updated or re-bind status, can be used to reply ARP request.
Your (client) IP address	4	Client IP address distributed by DHCP server.
Server IP address	4	IP address of DHCP server
Relay agent IP address	4	The first DHCP hop IP address after DHCP client sends request packets.
Client hardware address	16	Hardware address of DHCP client
Server host name	64	DHCP server name
File	128	DHCP client start up configuration file name and path assigned by DHCP server.
Options	Modifiable	A modifiable option field, including packet type, available leased period, DNS (Domain Name System) server IP address, WINS (Windows Internet Name Server) IP address, etc. information.

The A10E/A28E can be used as DHCP client to get IP address from DHCP server and management in future, as shown in Figure 3-5.

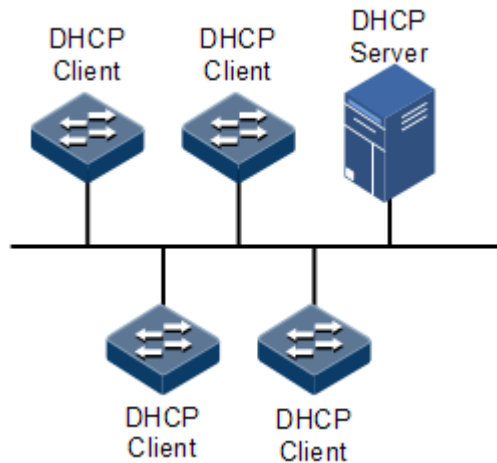


Figure 3-5 DHCP client networking

3.4.2 Preparing for configurations

Scenario

As a DHCP client, the A10E/A28E gets IP address assigned from the DHCP server.

The IP address assigned by DHCP client is limited with a certain lease period when adopting dynamic address distribution mode. DHCP server will take back the IP address when it is expired. DHCP client has to relet IP address for continuous use. DHCP client can release IP address if it does not want to use it any more before its expiration.

It is recommended that the number of DHCP relays be smaller than 4 if DHCP client needs to obtain IP address from DHCP server from multiple DHCP relays.

Prerequisite

- Create VLAN and add Layer 3 interface to it.
- Both DHCP snooping and DHCP Relay are disabled.

3.4.3 Default configurations of DHCP client

The default configuration of DHCP client is as below.

Function	Default value
hostname	alpha-a28e
class-id	alpha-a28e-ROS
client-id	alpha-a28e-SYSMAC-IF0

3.4.4 Applying the IP address through DHCP

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface ip if-number	Enter Layer 3 interface configuration mode.
3	Alpha-A28E(config-ip)# ip address dhcp vlan-list [server-ip ip-address]	Configure applying for the IP address through DHCP.



Note

If the A10E/A28E obtains IP address from the DHCP server through DHCP previously, it will restart the application process for IP address if users modified DHCP server address by the command of **ip address dhcp**.

3.4.5 (Optional) configuring DHCP client

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface ip if-number	Enter Layer 3 interface configuration mode.
3	Alpha-A28E(config)# ip dhcp client { class-id class-id client-id client-id hostname hostname }	Configure DHCP client information, including type ID, client ID, and host name.

3.4.6 (Optional) Renewing or releasing the IP address

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface ip if-number	Enter Layer 3 interface configuration mode.
3	Alpha-A28E(config)# ip dhcp client renew	Renew the IP address. If the A10E/A28E has obtained the IP address through DHCP, it will automatically renew the IP address upon the IP address expires.
4	Alpha-A28E(config)# no ip address dhcp	Release the IP address.

3.4.7 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show ip dhcp client	Show DHCP client configuration.

3.4.8 Configuring DHCP clients application

Networking requirements

As shown in Figure 3-6, the Switch is used as DHCP client, the host name is alpha-a28e. The DHCP server should assign IP address to SNMP interface of the Switch and make NMS platform manage the Switch.

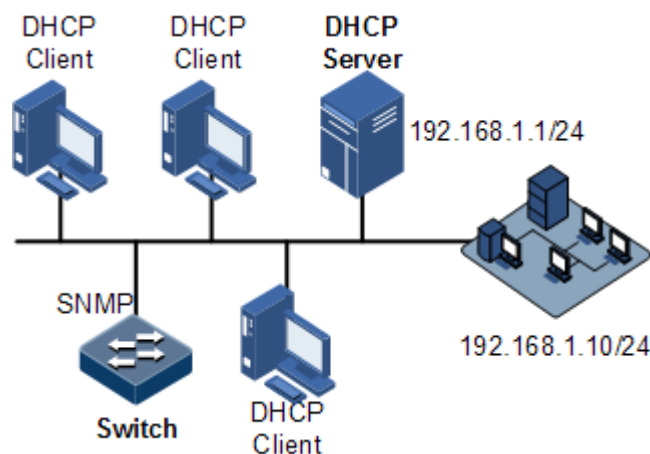


Figure 3-6 DHCP client networking

Configuration steps

Step 1 Configure DHCP client information.

```
Alpha-A28E#config
Alpha-A28E(config)#interface ip 0
Alpha-A28E(config-ip)#ip dhcp client hostname alpha-a28e
```

Step 2 Configure to apply for IP address by DHCP.

```
Alpha-A28E(config-ip)#ip address dhcp 1 server-ip 192.168.1.1
```

Checking results

Check whether DHCP client configuration is correct by the command of **show ip dhcp client**.

```
Alpha-A28E#show ip dhcp client
  Hostname:                alpha-a28e
  Class-ID:                alpha-a28eFTTH-ROS_4.14.1727
  Client-ID:               alpha-a28eFTTH-000e5e123456-IF0
  DHCP Client is requesting for a lease.
```

3.5 DHCP Relay

3.5.1 Introduction

At the beginning, DHCP requires that the DHCP server and clients must be in the same network segment. As a result, a DHCP server is configured for all network segments for dynamic host configuration, which is not economic.

DHCP Relay is introduced to solve this problem. It can provide relay service between DHCP clients and DHCP server that are in different network segments. It relays packets across network segments to the DHCP server or clients.

The working principle of DHCP Relay is shown below.

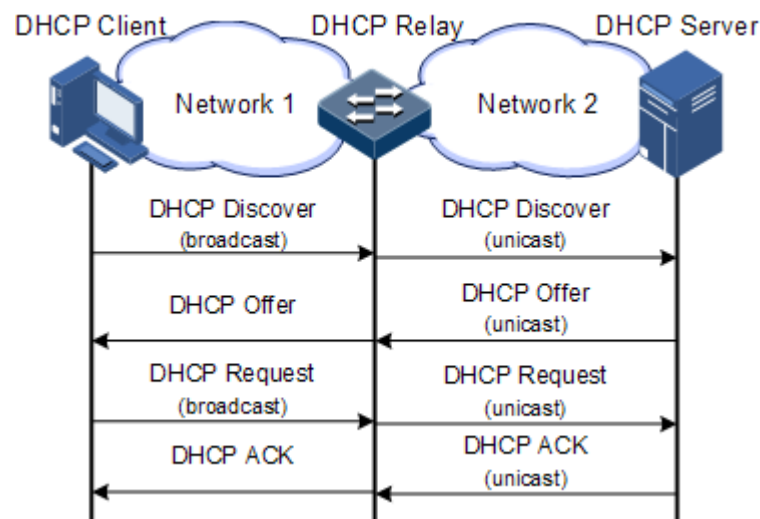


Figure 3-7 DHCP Relay application networking

- Step 1 The DHCP client sends a request packet to the DHCP server.
- Step 2 After receiving the packet, the DHCP relay device process the packet in a certain way, and then sends it to the DHCP server on the specified network segment.
- Step 3 The DHCP server sends acknowledgement packet to the DHCP client through the DHCP relay device according to the information contained in the request packet. In this way, the configuration of the DHCP client is dynamically configured.

3.5.2 Preparing for configurations

Scenario

When DHCP Client and DHCP Server are not in the same network segment, you can use DHCP Relay function to make DHCP Client and DHCP Server in different network segments carry relay service, and relay DHCP protocol packets across network segment to destination DHCP server, so that DHCP Client in different network segments can share the same DHCP Server.

Prerequisite

DHCP Relay is exclusive to DHCP Client, or DHCP Snooping. Namely, you cannot configure DHCP Relay on the device configured with DHCP Client, or DHCP Snooping.

3.5.3 Default configurations of DHCP Relay

Function	Default value
Global DHCP Relay	Disable
Interface DHCP Relay	Enable
DHCP Relay supporting Option 82	Disable
Policy for DHCP Relay to process Option 82 request packets	Replace
Interface DHCP Relay trust	No trust

3.5.4 Configuring global DHCP Relay

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip dhcp relay	Enable global DHCP Relay.

3.5.5 Configuring interface DHCP Relay

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface ip if-number	Enter Layer 3 interface configuration mode.
3	Alpha-A28E(config-ip)# ip dhcp relay	Enable DHCP Relay on the IP interface.

3.5.6 Configuring the destination IP address for forwarding packets

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip dhcp relay ip-list { all ip-interface-list } target-ip ip-address	Configuring the destination IP address for DHCP Relay on the IP interface.
3	Alpha-A28E(config)# interface ip if-number	Enter Layer 3 interface configuration mode.
4	Alpha-A28E(config-ip)# ip dhcp realy target-ip ip-address	Configure the destination IP address for Layer 3 interface to forward packets.

3.5.7 (Optional) configuring DHCP Relay to support Option 82

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip dhcp relay information option	Configure DHCP Relay to support Option 82.
3	Alpha-A28E(config)# ip dhcp relay information policy { drop keep replace }	Configure the policy for DHCP Relay to process Option 82 request packets
4	Alpha-A28E(config)# ip dhcp relay information trusted port-list port-list	Configure global Option 82 trusted interface list.
	Alpha-A28E(config)# interface port port-id Alpha-A28E(config-port)# ip dhcp relay information trusted	Set the specified interface to the Option 82 trusted interface.

3.5.8 Checking configurations

No.	Item	Description
1	Alpha-A28E# show ip dhcp relay [information statistics]	Show configurations or statistics of DHCP Relay.

3.6 DHCP Snooping

3.6.1 Introduction

DHCP Snooping is a security feature of DHCP with the below functions:

- Guarantee the DHCP client gets IP address from a legal DHCP server.

If a false DHCP server exists in the network, the DHCP client may obtain incorrect IP address and network configuration parameters, but cannot communicate normally. As shown below, to make DHCP client get IP address from the legal DHCP server, DHCP Snooping security system permits to set interface as trusted interface and untrusted interface: the trusted interface forwards DHCP packets normally; the untrusted interface discard the reply packets from the DHCP server.

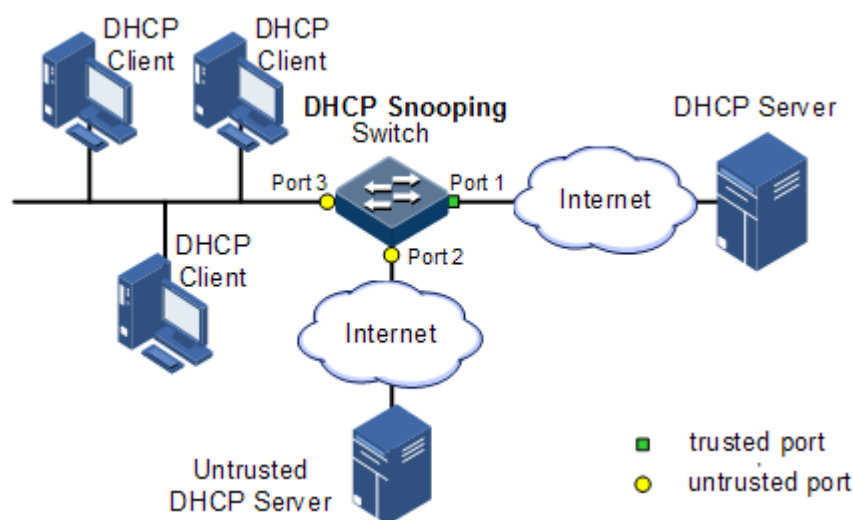


Figure 3-8 DHCP Snooping networking

- Record corresponding relationship between DHCP client IP address and MAC address.

The DHCP Snooping device records entries through monitor request and reply packets received by the trusted interface, including client MAC address, obtained IP address, DHCP client connected interface and VLAN of the interface, etc. Then implement following by the record information:

- ARP inspection: judge legality of user that sends ARP packet and avoid ARP attack from illegal user.
- IP Source Guard: filter interface forwarded packets by dynamically getting DHCP Snooping entry to avoid illegal packets pass the interface.
- VLAN mapping: packets sent to user modify mapped VLAN to original VLAN by searching mapped VLAN related DHCP client IP address, MAC address and original VLAN information in DHCP Snooping entry.

Option field in DHCP packet records position information of DHCP client. Administrator can use this option to locate DHCP client and control client security and accounting.

If the A10E/A28E configures DHCP Snooping to support Option function:

- When the A10E/A28E receives a DHCP request packet, deal with packets according to Option field included or not and filling mode as well as processing policy configured by user, then forwards the processed packet to DHCP server.

- When the A10E/A28E receives a DHCP reply packet, delete the field and forward to DHCP client if the packet does not contain Option field; forward packets directly if the packet does not contain Option field.

3.6.2 Preparing for configurations

Scenario

DHCP Snooping is a security feature of DHCP, being used to guarantee DHCP client gets IP address from legal DHCP server and record corresponding relationship between DHCP client IP and MAC address.

Option field of DHCP packet records location of DHCP client. Administrator can locate DHCP client through Option field and control client security and accounting. Device configured with DHCP Snooping and Option can perform related process according to Option field existence status in packet.

Prerequisite

DHCP Snooping is exclusive to DHCP Client, or DHCP Replay. Namely, you cannot configure DHCP Relay on the device configured with DHCP Client, or DHCP Snooping.

3.6.3 Default configurations of DHCP Snooping

The default configuration of DHCP Snooping is as below.

Function	Default value
Global DHCP Snooping status	Disable
Interface DHCP Snooping status	Enable
Interface trust/untrust status	Untrust
DHCP Snooping in support of Option 82	Disable

3.6.4 Configuring DHCP Snooping

Generally, make sure that the A10E/A28E interface connected to DHCP server is in trust state, while interface connected to user is in distrust state.

If enabling DHCP Snooping without configuring DHCP Snooping supporting Option function, the A10E/A28E will do nothing to Option fields in the packets. For packets without Option fields, the A10E/A28E still does not do insertion operation.

By default, the DHCP Snooping function of all interfaces is enabled, but only when global DHCP Snooping is enabled, the interface DHCP Snooping can take effect.

Configure DHCP Snooping over IPv4 on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# confi	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# ip dhcp snooping	Enable global DHCP Snooping. By default, global IPv4-based DHCP Snooping is not configured.
3	Alpha-A28E(config)# ip dhcp snooping port-list { all <i>port-list</i> }	(Optional) enable interface DHCP Snooping. By default, it is enabled.
4	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
5	Alpha-A28E(config-port)# ip dhcp snooping trust	Configure trust interface of DHCP Snooping. By default, the A10E/A28E does not trust DHCP packets received on the interface.
6	Alpha-A28E(config-port)# exit Alpha-A28E(config)# ip dhcp snooping information option	(Optional) configure DHCP Snooping to support Option 82 function.

3.6.5 Checking configurations

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# show ip dhcp snooping	Show configurations of DHCP Snooping.
2	Alpha-A28E# show ip dhcp snooping binding	Show configurations of DHCP Snooping binding table.

3.6.6 Example for configuring DHCP Snooping

Networking requirements

As shown in Figure 3-9, the switch is used as the DHCP Snooping device. The network requires DHCP clients to get IP address from a legal DHCP server and supports Option82 to facilitate client management; you can configure circuit ID sub-option information on Port 3 as alpha-a28e, and remote ID sub-option as user01.

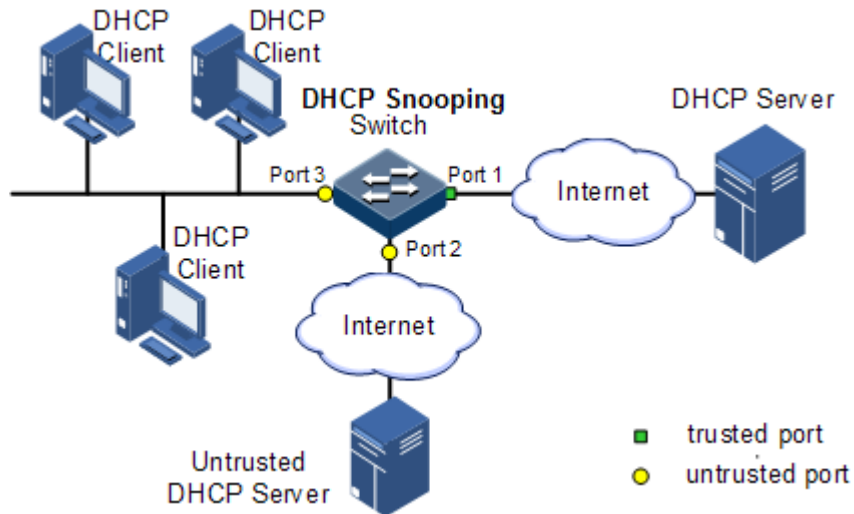


Figure 3-9 DHCP Snooping networking application

Configuration steps

Step 1 Configure global DHCP Snooping.

```
Alpha-A28E#config  
Alpha-A28E(config)#ip dhcp snooping
```

Step 2 Configure trust interface.

```
Alpha-A28E(config)#interface port 1  
Alpha-A28E(config-port)#ip dhcp snooping trust  
Alpha-A28E(config-port)#quit
```

Step 3 Configure DHCP Snooping to Option 82 function and configure the field Option 82.

```
Alpha-A28E(config)#ip dhcp snooping information option  
Alpha-A28E(config)#ip dhcp information option remote-id string user01  
Alpha-A28E(config)#interface port 3  
Alpha-A28E(config-port)#ip dhcp information option circuit-id alpha-a28e
```

Checking results

Use the **show ip dhcp information option** command to check whether DHCP snooping is correctly configured.

```
Alpha-A28E#show ip dhcp information option
```



```

DHCP Option Config Information
Attach-string:  alpha-a28e
Remote-ID Mode: string
Remote-ID String: user01
Port: 3   Circuit ID: alpha-a28e
    
```

3.7 DHCP options

3.7.1 Introduction

DHCP transmits control information and network configuration parameters through Option field in packet to realize address dynamical distribution so as to provide abundant network configuration information for client. DHCP protocol has 255 kinds of options, the final option is 255. Common used DHCP options are listed as below.

Table 3-2 Common DHCP options

Options	Description
3	Router option, to assign gateway for DHCP client
6	DNS server option, to assign DNS server address distributed by DHCP client
18	DHCP client flag option, to assign interface information for DHCP client
51	IP address lease option
53	DHCP packet type, to mark type for DHCP packets
55	Request parameter list option. Client uses this optical to indicate network configuration parameters need to obtain from server. The content of this option is values corresponding to client requested parameters.
60	Vendor ID option. The client and DHCP server can distinguish the vendor of the client by this option. The DHCP server can assign IP addresses in a specified range to client.
61	DHCP client flag option, to assign device information for DHCP client.
66	TFTP server name, to assign domain name for TFTP server distributed by DHCP client.
67	Start up file name, to assign start up file name distributed by DHCP client.
82	DHCP client flag option, user-defined, mainly used to mark position of DHCP client.
150	TFTP server address, to assign TFTP server address distributed by DHCP client.
184	DHCP reserved option, at present Option184 is mainly used to carry information required by voice calling. Through Option184 it can distribute IP address for DHCP client with voice function and meanwhile provide voice calling related information.

Options	Description
255	Complete option

Options 18, 61, and 82 in DHCP Option are relay agent information options in DHCP packets. When request packets from DHCP client arrive DHCP server, if need DHCP relay or DHCP snooping, DHCP relay or DHCP snooping increase Option field into request packets.

Options 18, 61, and 82 implement record DHCP client information on DHCP server. By cooperating with other software, it can realize IP address distribution restriction and accounting, etc. functions. Such as cooperate with IP Source Guard to defend deceive of IP address+MAC address.

Option 82 can include at most 255 sub-options. If defined field Option 82, at least one sub-option must be defined. The device supports two sub-option types currently: Sub-Option 1 (Circuit ID) and Sub-Option 2 (Remote ID).

- Sub-Option 1 contains interface ID of DHCP client request packet, interface VLAN and the additional information.
- Sub-Option 2 is interface MAC address (DHCP relay) or device bridge MAC address (DHCP snooping device) for receiving DHCP client request packets.

3.7.2 Preparing for configurations

Scenario

DHCP options 61, 82 are relay proxy information options in DHCP packet. When DHCP Client sends request packet to DHCP Server, DHCP snooping or DHCP relay will add Option field into request packet if it requires for DHCP snooping or DHCP relay.

DHCP Option 61, 82 fields are used to record DHCP client over IPv4. DHCP server cooperates with other software to implement functions such as IP address distribution restriction and accounting based on these information.

Prerequisite

N/A

3.7.3 Default configurations of DHCP Option

The default configuration of DHCP Option is as below.

Function	Default value
attach-string in global configuration mode	Null
remote-id in global configuration mode	switch-mac
circuit-id in interface configuration mode	Null

3.7.4 Configuring DHCP Option field

Configure DHCP snooping over IPv4 on the A10E/A28E as below.

All the following steps are optional and have not sequencing.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip dhcp information option attach-string <i>attach-string</i>	(Optional) configure additional information for Option 82 field.
3	Alpha-A28E(config)# interface port <i>port-id</i> Alpha-A28E(config-port)# ip dhcp information option circuit-id <i>circuit-id</i>	(Optional) configure circuit ID sub-option information for Option 82 field on the interface.
4	Alpha-A28E(config-port)# exit Alpha-A28E(config)# ip dhcp information option remote-id { client-mac client-mac-string hostname switch-mac switch-mac-string string <i>string</i> }	(Optional) configure remote ID sub-option information for Option 82 field.

3.7.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show ip dhcp information option	Show configurations of DHCP Option field.

4 QoS

This chapter introduces basic principle and configuration of QoS and provides related configuration applications, including the following chapters:

- Introduction
- Configuring basic QoS
- Configuring traffic classification and traffic policy
- Configuring priority mapping
- Configuring congestion management
- Configuring rate limiting based on interface and VLAN
- Configuring examples

4.1 Introduction

User brings force different service quality demands for network application, then network should distribute and schedule resource for different network application according to user demands. Quality of Service (QoS) can ensure service in real-time and integrity when network overload or congested and guarantee the whole network runs high-efficiently.

QoS is composed of a group of flow management technology:

- Service model
- Priority trust
- Traffic classification
- Traffic policy
- Priority mapping
- Congestion management

4.1.1 Service model

QoS technical service models:

- Best-effort Service
- Differentiated Services (DiffServ)

Best-effort

Best-effort service is the most basic and simplest service model over store and forward mechanism Internet (IPv4 standard). In Best-effort service model, the application program can send any number of packets at any time without permitting in advance and notifying the network. For Best-effort service, the network will send packets as possible as it can, but cannot guarantee the delay time and reliability.

Best-effort is the default Internet service model now, applying to most network applications, such as FTP, E-mail, etc. which is achieved by First In First Out (FIFO) queue.

DiffServ

DiffServ model is a multi-service model, which can satisfy different QoS requirements.

DiffServ model does not need to maintain state for each flow. It provides differentiated services according to the QoS classification of each packet. Many different methods can be used for QoS packet classification, such as IP packet priority (IP precedence), the packet source address or destination address and so on.

Generally, DiffServ is used to provide end to end QoS services for a number of important applications, which is achieved mainly through the following techniques:

- **CAR (Committed Access Rate):** CAR refers to classify the packets according to the pre-set packets matching rules, such as IP packets priority, the packet source address or destination address, etc. Continue to send the packets if the flow is in line with the rules of token bucket. If it is beyond the specified flow, discard the packets or remark IP precedence, DSCP, EXP, etc. CAR not only can control the flows, but also mark and remark the packets.
- **Queue technology:** the queuing technologies of SP, WRR, SP+WRR cache and schedule the congestion packets to achieve congestion management.

4.1.2 Priority trust

Priority trust refers to the A10E/A28E uses priority of packets for classification and performs QoS management.

The device supports packet priority trust based on interface, including:

- DSCP (Differentiated Services Code Point) priority
- CoS (Class of Service) priority
- Interface priority

4.1.3 Traffic classification

Traffic classification denotes recognizing packets of certain class by setting rules, performing different QoS policy for the packets match with different rules. It is premise and base of diverse service.

The A10E/A28E supports traffic classification by IP priority, DSCP priority and CoS priority over IP packets, as well as the classification by Access Control List (ACL) rule and VLAN ID. The traffic classification procedure is shown below.

CoS priority locates at the first 3 bits of TCI field, value range is 0–7, as shown below. It is available to guarantee service quality in Layer 2 network.

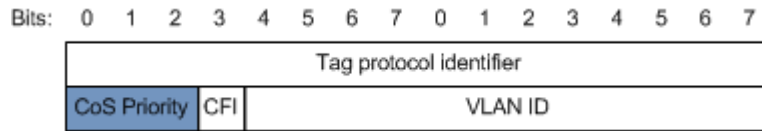


Figure 4-5 Structure of CoS priority packets

4.1.4 Traffic policy

Perform different operation for different packets after classifying packets flow, the traffic classification and operation binding form the traffic policy.

Rate limiting

Rate limiting is to control network flow, by monitoring flow rate enters network to discard overflow part and control the entering flow in a reasonable range, thus to protect network resource and carrier interest.

The A10E/A28E supports rate limiting based on traffic policy in the ingress direction on the interface.

The device supports to use token bucket for rate limiting, including single-token bucket and dual-token bucket.

Re-direction

Re-direction means to forward packets in the original corresponding relation between destination and interface, it forwards packet to assigned interface to implement policy routing.

The A10E/A28E supports redirect packets to the specified interface for forwarding in interface ingress direction.

Re-mark

Re-mark means to set some priority fields in packet again and then classify packets according to self-defined standard. Besides, downstream node in network can provide diverse QoS service according to re-marked information.

The device supports re-mark for below priority fields:

- IP packets IP priority
- DSCP priority
- CoS priority

Traffic statistics

Traffic statistics is used for data packets statistics of specified service flow, which is the number of packets and bytes passed through matching traffic classification or discarded.

Traffic statistics is not QoS control measure, but can be used in combination with other QoS actions to improve network supervision.

4.1.5 Priority mapping

When packets enter the A10E/A28E, priority mapping function sends them to queues with different internal priority in accordance with mapping relationship from external to internal, thus the packets can perform queue schedule at packets egress direction.

The device supports priority mapping over DSCP priority or CoS priority.

By default, the mapping relationship between device local priority and DSCP priority, local priority and CoS priority is shown below:

Table 4-1 Mapping relationship of local priority, DSCP priority, and CoS priority

Local priority	0	1	2	3	4	5	6	7
DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS	0	1	2	3	4	5	6	7

Local priority refers to a kind of packet priority with internal meaning assigned by the A10E/A28E, i.e. the priority corresponding to queue in QoS queue schedule.

Local priority range is 0-7; each interface of the A10E/A28E supports eight queues; local priority and interface queue is one-to-one corresponding relationship; the packet can be sent to assigned queue according to the mapping relationship between local priority and queue, as shown below.

Table 4-2 Mapping between local priority and queue

Local priority	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

4.1.6 Congestion management

Queue schedule is necessary when there is intermittent congestion in network or delay sensitive services require higher QoS service than non-sensitive services.

Queue schedule adopts different schedule algorithm to transport packets flow in queue. The device supports Strict Priority (SP), Weight Round Robin (WRR), and SP+WRR algorithm to solve network flow problem and have different influences on distribution, delay, and jitter of bandwidth resource.

- SP: to schedule strictly according to queue priority order. Lower priority queue cannot perform schedule until the packets in higher priority queue all finished schedule, as shown below.

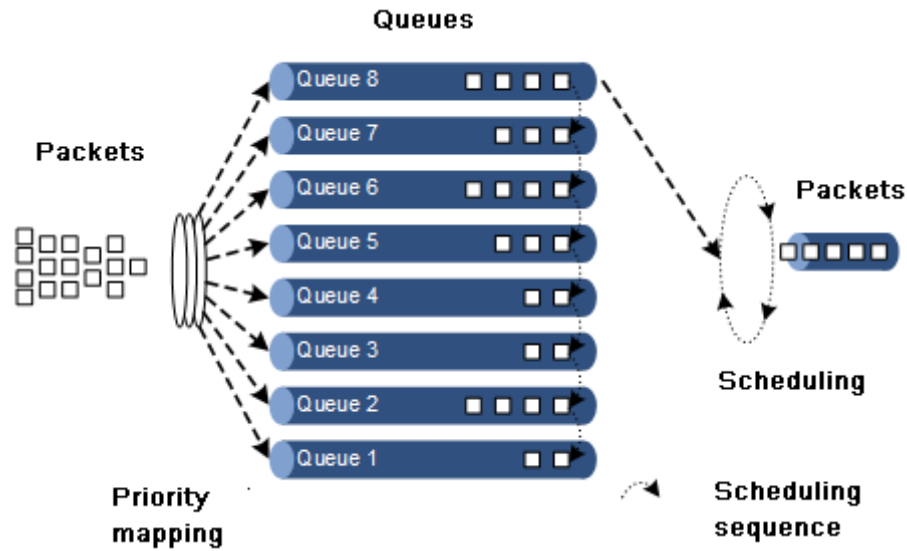


Figure 4-6 SP scheduling

- WRR: on basis of round schedule each queue according to queue priority, schedule packets in various queues according to weight of each queue, as shown in below.

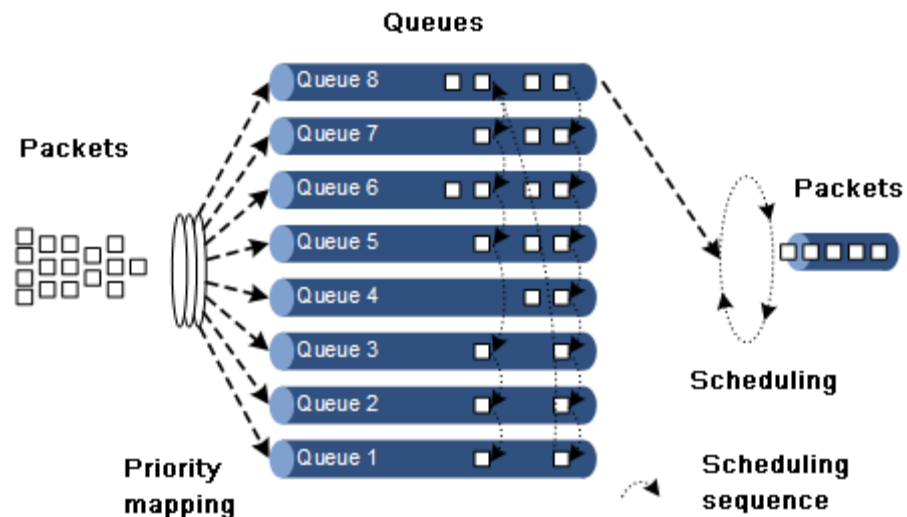


Figure 4-7 WRR scheduling

- SP+WRR: dividing queues on interface into two groups, you can assign some queues perform SP schedule and other queues perform WRR schedule.

4.1.7 Rate limiting based on interface and VLAN

The A10E/A28E not only supports rate limiting based on traffic policy but also supports rate limiting based on interface or VLAN ID. Similar to rate limiting based on traffic policy, the A10E/A28E discards the exceeding traffic.

4.2 Configuring basic QoS

4.2.1 Preparing for configurations

Scenario

Quality of Service (QoS) enables the carrier to provide different service quality for different applications, and assign and schedule different network resources.

Prerequisite

N/A

4.2.2 Default configurations of basic QoS

The default configuration of basic QoS is as below.

Function	Default value
Global QoS function status	Enable

4.2.3 Enabling global QoS

Enable global QoS function for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mls qos enable	Enable global QoS.

4.2.4 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show mls qos	Show global QoS status.

4.3 Configuring traffic classification and traffic policy

4.3.1 Preparing for configurations

Scenario

Traffic classification is the basis of QoS. You can classify packets from upstream device in accordance with priorities or ACL rule.

Traffic classification configuration will not take effect until user binds it to traffic policy. Applying traffic policy is related to network current loading condition and period. Usually, packets flow rate is limited according to configured speed when it enters network, and remark priority according to packet service feature.

Prerequisite

Enable global QoS.

4.3.2 Default configurations of traffic classification and traffic policy

The default configuration of traffic classification and traffic policy is as below.

Function	Default value
Traffic policy statistics function status	Disable

4.3.3 Creating traffic classification

Configure to create traffic classification on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# class-map <i>class-map-name</i> [match-all match-any]	Create traffic classification and enter traffic classification cmap configuration mode.
3	Alpha-A28E(config-cmap)# description <i>string</i>	(Optional) describe traffic classification.

4.3.4 Configuring traffic classification rules

Configure traffic classification rules on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# class-map <i>class-map-name</i> [match-all match-any]	Create traffic classification and enter traffic classification cmap configuration mode.
3	Alpha-A28E(config-cmap)# match { access-list-map ip- access-list mac-access- list } <i>acl-number</i>	(Optional) configure traffic classification over ACL rule. The ACL rule must be defined firstly and the type must be permit.
4	Alpha-A28E(config-cmap)# match class-map <i>class-map-name</i>	(Optional) configure traffic classification over traffic classification rule. The pursuant traffic classification must be created and the matched type must be identical with the traffic classification type.
5	Alpha-A28E(config-cmap)# match ip dscp <i>dscp-value</i>	(Optional) configure traffic classification over DSCP rules.
6	Alpha-A28E(config-cmap)# match ip precedence <i>precedence-</i> <i>value</i>	(Optional) configure traffic classification over IP priority.
7	Alpha-A28E(config-cmap)# match vlan <i>vlan-list</i> [double- tagging inner]	(Optional) configure traffic classification over VLAN ID rule of VLAN packets.



Note

- When the matched type of a traffic classification is **match-all**, the matched information may have conflict and the configuration maybe fails.
- Must configure traffic classification rule for traffic classification, i.e. take **match** configuration.
- For traffic classification quoted by traffic policy, you cannot modify traffic classification rule, namely, you cannot modify the **match** parameter of traffic classification.

4.3.5 Creating token bucket and rate limiting rules

Create rate limiting rule on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mls qos { aggregate-policer class-policer single-policer } <i>policer-name</i> <i>rate-</i> <i>value</i> <i>burst-value</i> [exceed-action { drop policed-dscp-transmit <i>dscp-</i> <i>value</i>]	Create token bucket and configure rate limiting rules.

4.3.6 Creating traffic policy

Configure to create traffic policy on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# policy-map <i>policy-map-name</i>	Create traffic policy and enter traffic policy pmap configuration mode.
3	Alpha-A28E(config- pmap)# description <i>string</i>	(Optional) configure traffic policy information.

4.3.7 Defining traffic policy mapping



Note

Define one or more defined traffic classifications to one traffic policy.

Configure to define traffic policy mapping on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# policy-map <i>policy-map-name</i>	Create traffic policy and enter traffic policy pmap configuration mode.
3	Alpha-A28E(config- pmap)# class-map <i>class-</i> <i>map-name</i>	Bind traffic classification into traffic policy; only apply traffic policy to packets matching with traffic classification. <div data-bbox="861 1299 1053 1388" data-label="Image"> </div> <div data-bbox="949 1339 1053 1382" data-label="Section-Header"> <h4>Note</h4> </div> <div data-bbox="877 1384 1382 1482" data-label="Text"> <p>At least one rule is necessary for traffic classification to bind traffic policy, otherwise the binding will fail.</p> </div>

4.3.8 Defining traffic policy operations





Note

Define different operations to different flows in policy.

Configure to define traffic policy operation on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# policy-map <i>policy-map-name</i>	Create traffic policy and enter traffic policy pmap configuration mode.
3	Alpha-A28E(config-pmap)# class-map <i>class-map-name</i>	Bind traffic classification into traffic policy; only apply traffic policy to packets matching with traffic classification.  Note At least one rule is necessary for traffic classification to bind traffic policy, otherwise the binding will fail.
4	Alpha-A28E(config-pmap-c)# police <i>policer-name</i>	(Optional) apply token bucket on traffic policy and take rate limiting and shaping.  Note The token bucket needs to be created in advance and configure rate limiting and shaping rule; otherwise, the operation will fail.
5	Alpha-A28E(config-pmap-c)# redirect-to <i>port port-id</i>	(Optional) configure re-direct rule under traffic classification, forwarding classified packets from assigned interface.
6	Alpha-A28E(config-pmap-c)# set { cos <i>cos-value</i> ip precedence <i>precedence-value</i> ip dscp <i>ip-dscp-value</i> vlan <i>vlan-id</i> }	(Optional) configure re-mark rule under traffic classification, modify packet CoS priority, DSCP priority, IP priority and VLAN ID.
7	Alpha-A28E(config-pmap-c)# copy-to-mirror	(Optional) configure flow mirror to monitor interface.
8	Alpha-A28E(config-pmap-c)# statistics enable	(Optional) configure flow statistic rule under traffic classification, statistic packets for matched traffic classification.

4.3.9 Applying traffic policy to interfaces

Configure to apply traffic policy to interface on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# service-policy <i>policy-name</i> ingress <i>port-id</i>	Bind the configured traffic policy with the interface.

4.3.10 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show service-policy statistics [<i>port port-id</i>]	Show traffic policy function status and the applied policy statistics.
2	Alpha-A28E# show class-map [<i>class-map-name</i>]	Show traffic classification information.
3	Alpha-A28E# show policy-map [<i>policy-map-name</i>]	Show traffic policy information.
4	Alpha-A28E# show policy-map [<i>policy-map-name</i>] [class <i>class-map-name</i>]	Show traffic classification information in traffic policy.
5	Alpha-A28E# show mls qos policer [<i>policer-name</i>]	Show assigned token bucket (rate limiting and shaping) information.
6	Alpha-A28E# show mls qos policer [aggregate-policer class-policer single-policer]	Show assigned type token bucket (rate limiting and shaping) information.
7	Alpha-A28E# show policy-map port [<i>port-id</i>]	Show traffic policy application information on the interface.
8	Alpha-A28E# show mls qos queue-rate [port-list port-list]	Show rate limiting on the interface.

4.3.11 Maintenance

Command	Description
Alpha-A28E(config)# clear service-policy statistics [egress <i>port-id</i> [class-map <i>class-map-name</i>] ingress <i>port-id</i> [class-map <i>class-map-name</i>] port <i>port-id</i>]	Clear statistics of QoS packets.

4.4 Configuring priority mapping

4.4.1 Preparing for configurations

Scenario

You can choose priority for trusted packets from upstream device, untrusted priority packets are processed by traffic classification and traffic policy. After configuring priority trust mode, the A10E/A28E operates packets according to their priorities and provides related service.

To specify local priority for packets is the prerequisite for queue scheduling. For packets from the upstream device, you cannot only map the external priority carried by packets to different local priority, but also configure local priority for packets based on interface, then the A10E/A28E will take queue scheduling according to local priority of packets. Generally speaking, IP packets need to configure mapping relationship between IP priority/DSCP priority and local priority; while VLAN packets need to configure mapping relationship between CoS priority and local priority.

Prerequisite

N/A

4.4.2 Default configurations of basic QoS

The default configuration of basic QoS is as below.

Function	Default value
Interface trust priority type	Trust CoS priority
Mapping from CoS to local priority	See Table 4-3.
Mapping from DSCP to local priority	See Table 4-4.
Interface priority	0

Table 4-3 Default CoS to local priority and color mapping relationship

CoS	0	1	2	3	4	5	6	7
Local	0	1	2	3	4	5	6	7

Table 4-4 Default DSCP to local priority and color mapping relationship

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
Local	0	1	2	3	4	5	6	7

4.4.3 Configuring interface trust priority type

Configure interface trust priority type for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.

Step	Configuration	Description
3	Alpha-A28E(config-port)#mls qos port-priority <i>priority</i>	Configure default priority on the interface.
4	Alpha-A28E(config-port)#mls qos trust { cos dscp port- priority }	Configure priority type of interface trust.

4.4.4 Configuring CoS to local priority

Configure mapping CoS to local priority for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E#config	Enter global configuration mode.
2	Alpha-A28E(config)#mls qos mapping cos <i>cos-value</i> to localpriority <i>priority</i>	Create mapping from CoS to local priority.

4.4.5 Configuring mapping from DSCP to local priority

Configure mapping from DSCP to local priority for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E#config	Enter global configuration mode.
2	Alpha-A28E(config)#mls qos mapping dscp <i>dscp-value</i> to local-priority <i>priority</i>	Create mapping from DSCP to local priority.

4.4.6 Configuring mapping from local priority to DSCP

Configure mapping from local priority to DSCP for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E#config	Enter global configuration mode.
2	Alpha-A28E(config)#policy-map <i>policy-map-name</i>	Create traffic policy and enter traffic policy pmap configuration mode.
3	Alpha-A28E(config-pmap)#class- map <i>class-map-name</i>	Bind traffic classification with traffic policy, and apply traffic policy to those packets that match traffic classification.
4	Alpha-A28E(config-pmap-c)#set local-priority <i>priority</i> Alpha-A28E(config-pmap-c)#exit Alpha-A28E(config-pmap)#exit	Configure local priority in pcmp-c mode, and return to global configuration mode.

Step	Configuration	Description
5	Alpha-A28E(config)# mls qos mapping local-priority priority to dscp dscp-value	Create mapping from local priority to DSCP.

4.4.7 Configuring all-traffic modification on the interface

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mls qos mapping local-priority to dscp enable	Enable mapping from local priority to DSCP.
3	Alpha-A28E(config)# mls qos non-modify port port-list	Configure the port list for disabling all-traffic modification.

4.4.8 Configuring specific-traffic modification

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# policy-map policy-map-name	Create traffic policy and enter traffic policy pmap configuration mode.
3	Alpha-A28E(config-pmap)# class-map class-map-name	Bind traffic classification with traffic policy, and apply traffic policy to those packets that match traffic classification.
4	Alpha-A28E(config-pmap-c)# modify enable	Enable specific-traffic modification.

4.4.9 Configuring CoS copying

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# switchport qinq dot1q-tunnel	(Optional) enable basic QinQ functions.

Step	Configuration	Description
4	Alpha-A28E(config-port)# switchport vlan-mapping <i>vlan-id add-outer</i> <i>vlan-id</i>	(Optional) enable selective QinQ functions.
5	Alpha-A28E(config-port)# switchport vlan-mapping ingress <i>vlan-id</i> translate <i>vlan-id</i>	(Optional) enable VLAN mapping.
6	Alpha-A28E(config-port)# exit	Return to global configuration mode.
7	Alpha-A28E(config)# m1s qos cos-remark enable	Enable CoS copying.

4.4.10 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show m1s qos	Show global QoS status.
2	Alpha-A28E# show m1s qos port [<i>port-id</i>]	Show interface QoS priority, and trust mode information.
3	Alpha-A28E# show m1s qos mapping cos	Show information about mapping from CoS to local priority.
4	Alpha-A28E# show m1s qos mapping dscp	Show information about mapping from DSCP to local priority.
5	Alpha-A28E# show m1s qos mapping localpriority	Show information about mapping from local priority to queue.
6	Alpha-A28E# show m1s qos localpriority-to-dscp	Show information about mapping from local priority to DSCP.

4.5 Configuring congestion management

4.5.1 Preparing for configurations

Scenario

When network has congestion, user want to balance delay and delay jitter of various packets, packets of key services (like video and voice) can be processed preferentially; packets of secondary services (like E-mail) with identical priority can be fairly processed, different priority can be processed according to its weight value. You can configure queue schedule in this situation. Selection of schedule algorithm is depended on service condition and customer requirements.

Prerequisite

Enable global QoS.

4.5.2 Default configurations of congestion management

The default configuration of congestion management is as below.

Function	Default value
Queue schedule mode	SP
Queue weight	WRR weight for scheduling 8 queues is 1.

4.5.3 Configuring SP queue scheduling

Configure SP queue schedule on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# m1s qos queue scheduler sp	Configure interface queue scheduling mode as SP.

4.5.4 Configuring WRR or SP+WRR queue scheduling

Configure WRR or SP+WRR on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# m1s qos queue scheduler wrr	Configure interface queue schedule mode as WRR.
3	Alpha-A28E(config-port)# m1s qos queue wrr weigh1 weight2 weight3...weight8	Configure weight for each queue. Perform SP scheduling when the priority of a queue is 0.

4.5.5 Configuring queue transmission rate

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.

Step	Configuration	Description
3	Alpha-A28E(config-port)# m1s qos queue-rate [queue-list queue-list] min rate-limit max rate-limit	Configure interface-based queue transmission rate.

4.5.6 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show m1s qos port [port-id]	Show QoS priority and trust mode on the interface.
2	Alpha-A28E# show m1s qos queue	Show queue weight information.
3	Alpha-A28E# show m1s qos queue-rate [port-list port-list]	Show interface-based queue transmission rate.

4.6 Configuring rate limiting based on interface and VLAN

4.6.1 Preparing for configurations

Scenario

When the network has congestion, you want to restrict burst flow on some interface, or some VLAN to make it transmit in a well-proportioned rate so as to remove network congestion. You need to configure rate limiting based on interface or VLAN

Prerequisite

Related VLAN must be created before configuring rate limiting based on VLAN or QinQ.

4.6.2 Configuring rate limiting based on interface

Configure rate limiting based on interface on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# rate-limit port-list { all port-list } { egress ingress } rate-value [burst-value]	Configure rate limiting based on interface.
	Alpha-A28E(config)# rate-limit port-list { all port-list } both rate-value	

4.6.3 Configuring rate limiting based on VLAN

Configure rate limiting based on VLAN on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# rate-limit vlan <i>vlan-id</i> <i>rate-value</i> <i>burst-value</i> [statistics]	(Optional) configure rate limiting based on VLAN.

4.6.4 Configuring rate limiting based on QinQ

Configure rate limiting based on QinQ on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# rate-limit double-tagging-vlan outer { <i>outer-vlan-id</i> any } inner { <i>inner-vlan-id</i> any } <i>rate-value</i> <i>burst-value</i> [statistics]	(Optional) configure rate limiting based on QinQ.

4.6.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show rate-limit port-list [<i>port-list</i>]	Show configurations of rate limiting on specified interfaces.
2	Alpha-A28E# show rate-limit vlan	Show configurations of rate limiting based on VLAN.

4.6.6 Maintenance

Maintain the A10E/A28E as below.

Command	Description
Alpha-A28E(config)# clear rate-limit statistics vlan [<i>vlan-id</i>]	Clear statistics of packet lost due to rate limiting based on VLAN.

4.7 Configuring examples

4.7.1 Example for configuring congestion management

Networking requirements

As shown below, the user uses voice, video and data services.

CoS priority of voice service is 5, CoS priority of video service is 4, CoS priority of data service is 2. The local priorities for these three types of services are mapping 6, 5, and 2 respectively.

It is easy for Switch A to occur congestion, for reduce network congestion; user needs to make the following rules according to different services types:

- For voice service, perform SP schedule to make sure this part of flow passes through in prior;
- For video service, perform WRR schedule, with weight value 50;
- For data service, perform WRR schedule, with weight value 20;

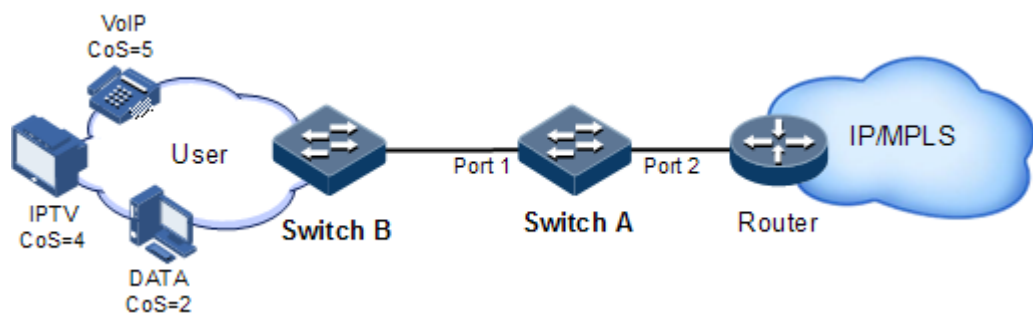


Figure 4-8 Configure queue schedule networking

Configuration steps

Step 1 Configure interface priority trust mode.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#mls qos enable
SwitchA(config)#interface port 2
SwitchA(config-port)#mls qos trust cos
SwitchA(config-port)#quit
```

Step 2 Configure mapping profile between CoS priority and local priority.

```
SwitchA(config)#mls qos mapping cos 5 to local-priority 6
SwitchA(config)#mls qos mapping cos 4 to local-priority 5
SwitchA(config)#mls qos mapping cos 2 to local-priority 2
```

Step 3 Configure to take SP+WRR queue schedule on Port 1 egress direction.

```
SwitchA(config)#mls qos queue wrr 1 1 20 1 1 50 0 0
```

Checking results

Show interface priority trust mode.

```
SwitchA#show mls qos port 2
Port      Priority  Trust      Flow Modify
-----
2         0        Cos       Enable
...
```

Check whether mapping relationship between Cos priority and local priority is correctly configured.

```
SwitchA#show mls qos mapping cos
CoS-LocalPriority Mapping:
          CoS:  0  1  2  3  4  5  6  7
-----
LocalPriority: 0  1  2  3  5  6  6  7
```

```
SwitchA#show mls qos mapping localpriority
LocalPriority-Queue Mapping:
LocalPriority: 0  1  2  3  4  5  6  7
-----
Queue: 1  2  3  4  5  6  7  8
```

Check whether queue scheduling is correctly configured on the interface.

```
SwitchA#show mls qos queue
Queue    weight(WRR)
-----
1        1
2        1
3        20
4        1
5        1
6        50
7        0
8        0
```


4.7.2 Example for configuring rate limiting based on interface

Networking requirements

As shown below, User A, User B, User C are respectively connected to Switch A, Switch B, Switch C and A10E/A28E.

User A requires voice and video services, User B requires voice, video and data services, User C requires video and data services.

According to service requirements, user needs to make rules as below.

- For User A, provide 25 Mbit/s assured bandwidth, permitting burst flow 100 KB and discarding redundant flow;
- For User B, provide 35 Mbit/s assured bandwidth, permitting burst flow 100 KB and discarding redundant flow;
- For User C, provide 30 Mbit/s assured bandwidth, permitting burst flow 100 KB and discarding redundant flow.

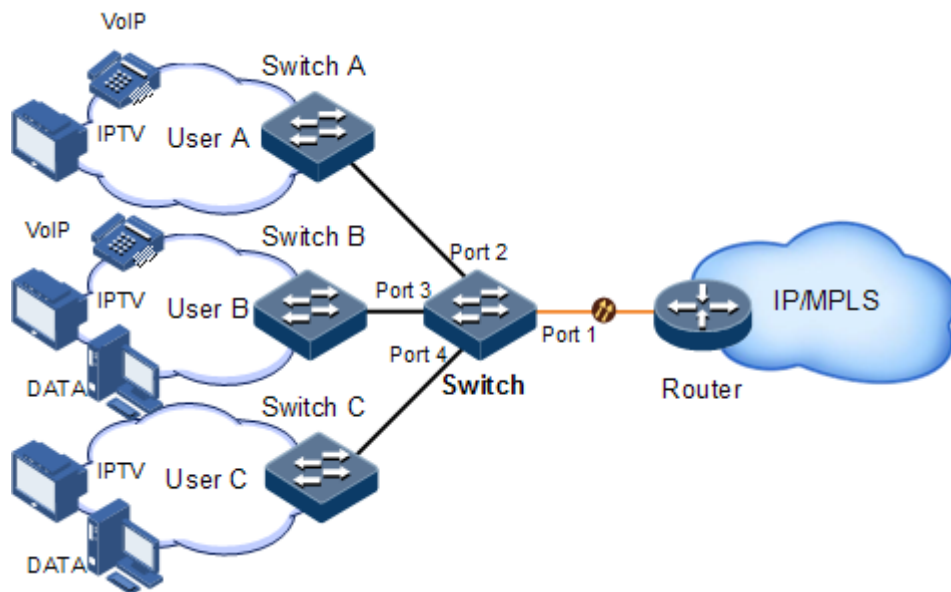


Figure 4-9 Rate limiting based on interface

Configuration steps

Step 1 Configure rate limiting based on interface.

```
Alpha-A28E#config
Alpha-A28E(config)#rate-limit port-list 2 ingress 25000 100
Alpha-A28E(config)#rate-limit port-list 3 ingress 35000 100
Alpha-A28E(config)#rate-limit port-list 4 ingress 30000 100
```

Checking results

Show rate limiting configuration based on interface by the command of **show rate-limit interface-type interface-number**.

Alpha-A28E#**show rate-limit port-list 2-4**

I-Rate: Ingress Rate

I-Burst: Ingress Burst

E-Rate: Egress Rate

E-Burst: Egress Burst

Port	I-Rate(kbps)	I-Burst(kB)	E-Rate(kbps)	E-Burst(kB)
2	24992	100	0	0
3	34976	100	0	0
4	29984	100	0	0

5 Multicast

This chapter introduces basic principle and configuration of multicast and provides related configuration applications, including the following chapters:

- Overview
- Configuring IGMP Snooping
- Configuring MVR
- Configuring MVR Proxy
- Configuring IGMP filtering
- Maintenance
- Configuration examples

5.1 Overview

With the continuous development of Internet network, the various interacting network data, voice and video will become more and more; the other hand, the emerging e-commerce, online meetings, online auctions, video on demand, distance learning and other services also rise gradually. These services come up with higher requirements for network bandwidth, information security and paid. Traditional unicast and broadcast cannot meet these requirements well, while multicast has met them timely.

Multicast is a point to multipoint data transmission method. The method can effectively solve the single point sending and multipoint receiving problems. During the network packet transmission, it can save network resources and improve information security.

Basic concept in multicast

- Multicast group

Multicast group refers to the recipient set using the same IP multicast address identification. Any user host (or other receiving device) will become a member of the group after joining the multicast group. They can identify and receive multicast data with the destination address of IP multicast address.

- Multicast group members

All hosts joined a multicast group will become a member of the multicast group. Multicast group members are dynamic, hosts can join or leave multicast group at any time. Group members may be widely distributed in any part of the network.

- Multicast source

Multicast source refers to a server which regards multicast group address as the destination address to send IP packet. A multicast source can send data to multiple multicast groups; multiple multicast sources can send to a multicast group.

- Multicast router

The router that supports Layer 3 multicast is called the multicast router. Multicast router can achieve multicast routing, guide multicast packet forwarding and provide multicast group management function to distal network segment connecting with users.

- Router interface

The router interface is also called source interface. It refers to the interface toward multicast router between multicast router and the host. The A10E/A28E receives multicast packets from this interface.

- Member interface

Known as the receiving interface, the member interface is the interface toward host between multicast router and the host. The A10E/A28E sends multicast packets from this interface.

Multicast address

In order to make multicast source and multicast group members communicate across the Internet, you need to provide network-layer multicast address and link-layer multicast address, i.e. IP multicast address and multicast MAC address. Note: multicast address only can be destination address, but not source address.

- IP multicast address

IANA (Internet Assigned Numbers Authority) assigns Class D address space to IPv4 multicast; the range of IPv4 multicast address is from 224.0.0.0 to 239.255.255.255.

- Multicast MAC address

When Ethernet transmits unicast IP packet, the destination MAC address will use the recipient MAC address. However, when multicast packets are in transmission, the destination is no longer a specific receiver, but a group with uncertain member, so it needs to use multicast MAC address.

Multicast MAC address for link layer identifies the receiver of the same multicast group.

According to IANA, the high 24-bit of multicast MAC address are 0x01005E, the 25-bit is fixed 0, the 23-bit corresponds to the low 23-bit of IPv4 multicast address.

The mapping relation between IP multicast address and MAC address is shown below.

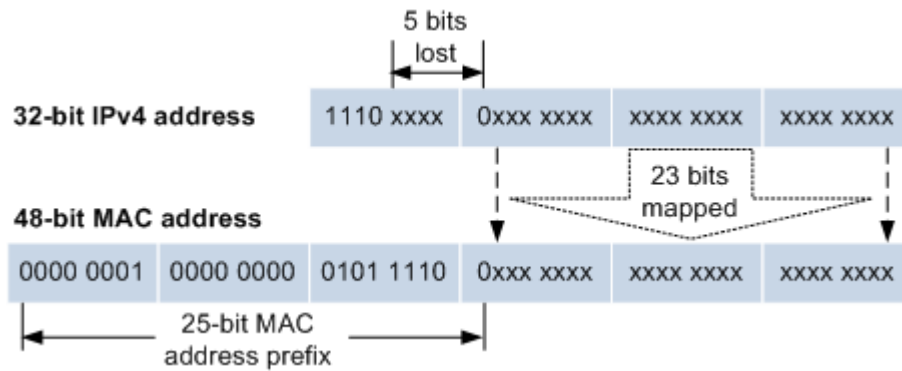


Figure 5-1 Mapping relation between IPv4 multicast address and multicast MAC address

Since the first 4 bits of IP multicast address are 1110, indicating multicast identification. In the last 28bits, only 23 bits are mapped to the multicast MAC address. And the missing 5 bits information will make 32 IP multicast addresses map to the same multicast MAC address. Therefore, in Layer 2, the A10E/A28E may receive some other data out of IPv4 multicast group, and these extra multicast data need to be filtered by the upper device.

Supported multicast features

The A10E/A28E supports the following multicast features:

- Internet Group Management Protocol Snooping (IGMP) Snooping
- Multicast VLAN Registration (MVR)
- MVR Proxy
- IGMP filtering



Note

- MVR Proxy is usually used with MVR.
- IGMP filtering can be used with IGMP Snooping or MVR.

5.1.2 IGMP Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is multicast constraining mechanism running on Layer-2 devices, used for multicast group management and control and achieve Layer 2 multicast.

IGMP Snooping allows a Layer 2 device to monitor IGMP session between hosts and multicast routers. When monitoring a group of IGMP Report from host, the Layer 2 device will add host-connected interface to the forwarding entry of this group. Similarly, when forwarding entry reaches aging time, the Layer 2 device deletes host-connected interface from forwarding entry.

IGMP Snooping forwards multicast data by Layer 2 multicast forwarding entry. When receiving multicast data, the Layer 2 device forwards them directly according to the corresponding receiver interface of multicast forwarding entry, but not flood to all interfaces, so as to save the switch bandwidth effectively.

IGMP Snooping establishes Layer 2 multicast forwarding entry, which can be learnt dynamically or configured manually.



Note

Currently, the switch supports up to 1024 Layer 2 multicast entries.

5.1.3 MVR

MVR (Multicast VLAN Registration) is multicast constraining mechanism running on Layer 2 devices, used for multicast group management and control and achieve Layer 2 multicast.

MVR adds member interfaces belonging to different user VLANs on the Layer device to multicast VLAN by configuring multicast VLAN and makes different VLAN user uses one common multicast VLAN, then the multicast data will be transmitted only in one multicast VLAN without copying one for each user VLAN, thus saving bandwidth. At the same time, multicast VLAN and user VLAN are completely isolated which also increases the security.

Both MVR and IGMP Snooping can achieve Layer 2 multicast, but the difference is: Multicast VLAN in IGMP Snooping is the same with user VLAN, while multicast VLAN in MVR can be different with user VLAN.



Note

One switch can be configured with up to 10 multicast VLAN, at least one multicast VLAN and group addresses. It supports up to 1024 multicast groups.

5.1.4 MVR Proxy

MVR Proxy is an MVR protocol proxy mechanism. It runs on Layer 2 devices to assist in managing and controlling multicast groups. MVR Proxy will terminate IGMP packets; It can proxy host function and also proxy multicast router functions for the next agent. The Layer 2 network device enabled with MVR Proxy has two roles:

- On the user side, it is a query builder and undertakes the role of Server, sending Query packets and periodically checking user information, and dealing with the Report and Leave packets from user.
- On the network routing side, it is a host and undertakes the role of Client, responding the multicast router Query packet and sending Report and Leave packets. It sends the user information to the network when they are in need.

The proxy mechanism can control and access user information effectively, at the same time, reducing the network side protocol packet and network load.

MVR Proxy establishes the multicast forwarding table by blocking IGMP packets between users and the multicast router.



Note

MVR Proxy is usually used with MVR.

The following concepts are related to MVR Proxy.

- IGMP packet suppression

IGMP packet suppression refers that the Layer 2 device filters identical Report packets. When receiving Report packets from a multicast group member in a query interval, the Layer 2 device sends the first Report packet to the multicast router only rather than other identical Report packets, to reduce packet quantity on the network.



Note

When MVR is enabled, IGMP packet suppression can be enabled or disabled respectively.

- IGMP Querier

If a Layer 2 device is enabled with this function, it can actively send IGMP query packets to query information about multicast members on the interface. If it is disabled with this function, it only forwards IGMP query packets from routers.



Note

When IGMP Snooping is enabled, IGMP Querier can be enabled or disabled respectively.

- Source IP address of query packets sent by IGMP Querier

IGMP querier sends the source IP address of query packets. By default, the IP address of IP interface 0 is used. If the IP address is not configured, 0.0.0.0 is used. When receiving query packets with IP address of 0.0.0.0, some hosts take it illegal and do not respond. Thus, specifying the IP address for the query packet is recommended.

- Query interval

It is the query interval for common groups. The query message of common group is periodically sent by the Layer 2 device in multicast mode to all hosts in the shared network segment, to query which multicast groups have members.

- Maximum response time for query packets

The maximum response time for query packets is used to control the deadline for reporting member relations by a host. When the host receives query packets, it starts a timer for each added multicast group. The value of the timer is between 0 and maximum response time. When the timer expires, the host sends the Report packet to the multicast group.

- Interval for last member to send query packets

It is also called the specified group query interval. It is the interval for the Layer 2 device continues to send query packets for the specified group when receiving IGMP Leave packet for a specified group by a host.

The query packet for the specified multicast group is sent to query whether the group has members on the interface. If yes, the members must send Report packets within the maximum response time; after the Layer 2 device receives Report packets in a specie period, it continues to maintain multicast forwarding entries of the group; If the members fail to send Report packets within the maximum response time, the switch judges that the last member of the multicast group has left and thus deletes multicast forwarding entries.

5.1.5 IGMP filtering

To control user access, you can set IGMP filtering. IGMP filtering contains the range of accessible multicast groups passing filtering rules and the maximum number of groups.

- IGMP filtering rules

To ensure information security, the administrator needs to limit the multicast users, such as what multicast data are allowed to receive and what are not.

Configure IGMP Profile filtering rules to control the interface. One IGMP Profile can be set one or more multicast group access control restrictions and access the multicast group according to the restriction rules (**permit** and **deny**). If a rejected IGMP Profile filter profile is applied to the interface, the interface will discard the IGMP report packet from this group directly once receiving it and does not allow receiving this group of multicast data.

IGMP filtering rules can be configured on interface or VLAN.

IGMP Profile only applies to dynamic multicast groups, but not static ones.

- Limit to the maximum number of multicast group

The maximum allowed adding number of multicast group and the maximum group limitation rule can be set on interface or interface+VLAN.

The maximum group limitation rule sets the actions for reaching the maximum number of multicast group users added, which can be no longer allowing user adding groups, or covering the original adding group.



IGMP filtering is usually used with MVR.

5.2 Configuring IGMP Snooping

5.2.1 Preparing for configurations

Scenario

Multiple hosts belonging to the same VLAN receive data from the multicast source. Enable IGMP Snooping on the Layer 2 device that connects the multicast router and hosts. By listening IGMP packets transmitted between the multicast router and hosts, creating and maintaining the multicast forwarding table, you can implement Layer 2 multicast.

Prerequisite

Create a VLAN, and add related interfaces to the VLAN.

5.2.2 Default configurations of IGMP Snooping

Function	Default value
Global IGMP Snooping status	Disable
VLAN IGMP Snooping status	Disable
Aging time of router interface and multicast forwarding entry in IGMP Snooping	300s

5.2.3 Enabling global IGMP Snooping

Step	Function	Default value
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip igmp snooping	Enable global IGMP Snooping.

5.2.4 (Optional) enabling IGMP Snooping on VLANs

When global IGMP Snooping is enabled, IGMP Snooping is enabled on all VLANs by default. In this situation, you can disable or re-enable IGMP Snooping on a VLAN in VLAN configuration mode.

When global IGMP Snooping is disabled, IGMP Snooping is disabled on all VLANs by default. In this situation, you cannot enable IGMP Snooping on a VLAN.

Configuring IGMP Snooping in VLAN configuration mode

In VLAN configuration mode, you can enable IGMP Snooping on only one VLAN at a time.

Step	Function	Default value
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# vlan <i>vlan-id</i>	Enable VLAN configuration mode.
3	Alpha-A28E(config-vlan)# ip igmp snooping	Enable IGMP Snooping on a VLAN.

Configuring IGMP Snooping in global configuration mode

In VLAN configuration mode, you can enable IGMP Snooping on multiple VLANs at a time.

Step	Function	Default value
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip igmp snooping vlan-list <i>vlan-list</i>	Enable IGMP Snooping on VLANs.

5.2.5 Configuring the multicast router interface

Step	Function	Default value
1	Alpha-A28E# config	Enter global configuration mode.

Step	Function	Default value
2	Alpha-A28E(config)# ip igmp snooping mrouter vlan <i>vlan-id</i> port-list <i>port-list</i>	Configure the multicast router interface of the specified VLAN.



Note

- IGMP Snooping can dynamically learn router interfaces (on the condition that the multicast router is enabled with multicast route protocol, and through IGMP query packets), or you can manually configure dynamic learning so that downstream multicast report and leaving packets can be forwarded to the router interface.
- There is aging time for the router interface dynamically learnt and no aging time for manually configured router interface.

5.2.6 (Optional) configuring the aging time of IGMP Snooping

For IGMP Snooping, each dynamically learnt router interface initiates a timer, of which the expiration time is the aging time of IGMP Snooping. When the timer expires, the route interface will no longer be a router interface if it has not received IGMP Query packet, or it updates the aging time if it receives IGMP Query packet.

Each multicast forwarding entry initiates a timer which contains the aging time of a multicast member. The expiration time of the timer is the aging time of IGMP Snooping. When the timer expires, the multicast member will be deleted if it has not received IGMP Report packet, or it updates the aging time if it receives IGMP Report packet.

Step	Function	Default value
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip igmp snooping timeout { <i>period</i> infinite }	Configure the aging time of router interface and multicast forwarding entry of IGMP Snooping.



Note

The aging time of IGMP Snooping configured by the previous command takes effects on all dynamically learnt router interfaces and multicast forwarding entries on the A10E/A28E.

5.2.7 (Optional) configuring instance leaving

For IGMP Snooping, when a user sends a Leave packet, the A10E/A28E does not immediately delete the corresponding multicast forwarding entry, but deletes it until the aging time of the entry expires. When downstream users are in a large number, and they join or leave the network frequently, you can configure this function to immediately delete corresponding multicast forwarding entries.

Configuring immediate leaving in VLAN configuration mode

In VLAN configuration mode, you can enable instance leaving on only one VLAN at a time.

Step	Function	Default value
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# vlan <i>vlan-id</i>	Enable VLAN configuration mode.
3	Alpha-A28E(config-vlan)# ip igmp snooping immediate-leave	Configure instance leaving on the VLAN.

Configuring IGMP Snooping in global configuration mode

In VLAN configuration mode, you can configure immediate leaving on multiple VLANs at a time.

Step	Function	Default value
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip igmp snooping vlan-list <i>vlan-list</i> immediate-leave	Configure immediate leaving on VLANs.

5.2.8 (Optional) configuring static multicast forwarding table

An interface is added to the multicast group through the IGMP Report packet sent by a host. Or you can manually add an interface to a multicast group.

Step	Function	Default value
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mac-address-table static multicast <i>mac-address</i> vlan <i>vlan-id</i> port-list <i>port-list</i>	Add interfaces to the static multicast group.

5.2.9 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show ip igmp snooping [vlan <i>vlan-id</i>]	Show configurations of IGMP Snooping.

No.	Item	Description
2	Alpha-A28E# show ip igmp snooping mrouter [<i>vlan vlan-id</i>]	Show information about multicast router interface of IGMP Snooping.
3	Alpha-A28E# show mac-address-table multicast [<i>vlan vlan-id</i>] [<i>count</i>]	Show information about Layer 2 multicast MAC address table.

5.3 Configuring MVR

5.3.1 Preparing for configurations

Scenario

Multiple hosts receive data from the multicast sources. These hosts and the multicast router belong to different VLANs. Enable MVR on Switch A, and configure multicast VLAN. In this way, users in different VLANs can share a multicast VLAN to receive the same multicast data, and reduce bandwidth waste.

Prerequisite

Create VLANs and add related interfaces to VLANs.


5.3.2 Default configurations of MVR

Function	Default value
Global MVR status	Disable
Interface MVR status	Disable
Multicast VLAN and group address set	None
MVR multicast entity aging time	600s
MVR operation mode	Dynamic
MVR interface immediate leaving status	Disable

5.3.3 Configuring MVR basic information

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# mvr enable	Enable global MVR.
3	Alpha-A28E(config)# mvr timeout period	(Optional) configure the aging time of MVR multicast entities.
4	Alpha-A28E(config)# mvr vlan vlan-id	Configure MVR multicast VLAN.
5	Alpha-A28E(config)# mvr vlan vlan-id group ip-address [count]	Configure group address set for multicast VLAN.  Note The mvr vlan vlan-id group ip-address [count] command is used to configure group address set for multicast VLAN. If the received IGMP Report packet does not belong to group address set of any VLAN, it is not processed and the user cannot make multicast traffic on demand.
6	Alpha-A28E(config)# mvr mode { compatible dynamic }	(Optional) configure MVR operation mode. Wherein, the dynamic mode allows source interfaces to dynamically join the multicast group; the compatible mode does not allow source interfaces to dynamically join the multicast group. Only when the receiving interface has a member which joins the multicast group, the source interface can join the multicast group.

5.3.4 Configuring MVR interface information



Caution

On an aggregating device, configuring immediate leaving is not commended on the receiving interface. If multiple users are connected to the receiving interface configured with immediate leaving through another device, the aggregating device will delete the receiving interface. As a result, other users that are still connected to the receiving interface fail to receive multicast traffic.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mvr enable	Enable global MVR.
3	Alpha-A28E(config)# interface interface-type interface-number	Enter physical layer interface configuration mode.

Step	Configuration	Description
4	Alpha-A28E(config-port)#mvr	(Optional) enable interface MVR.
5	Alpha-A28E(config-port)#mvr type { receiver source }	Configure the type of interface MVR. By default, the type is non-MVR. To configure it, set the uplink interface to the source interface to receive multicast data. Users cannot be directly connected to the source interface; all source interfaces must be in the multicast VLAN; set the interface directly connected to the user to the receiving interface and it cannot belong to the multicast VLAN.
6	Alpha-A28E(config-port)#mvr immediate	(Optional) configure immediate leaving on the MVR interface. This function can be applied to the receiving interface directly connected to the user.



Note

After global MVR is enabled, interface MVR is enabled as well.

5.3.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E#show mvr	Show configurations of MVR.
2	Alpha-A28E#show mvr vlan group [vlan vlan-6.3 id]	Show MVR multicast VLAN and group address set.
3	Alpha-A28E#show mvr vlan vlan-id member	Show information about MVR multicast member.

5.4 Configuring MVR Proxy

5.4.1 Preparing for configurations

Scenario

In a network with multicast routing protocol widely applied, there are multiple hosts and client subnet receiving multicast information. Enable IGMP Proxy on the Layer 2 device that connects the multicast router and hosts, to block IGMP packets between hosts and the multicast router and relieve the network load.

Configure IGMP Proxy to relive configuration and management of client subnet for the multicast router and to implement multicast connection with the client subnet.

Prerequisite


- Enable MVR.
- Configure multicast VLAN and group address set.
- Configure the source interface and the receiving interface, and add related interfaces to the corresponding VLANs.

5.4.2 Default configurations of IGMP Proxy

Function	Default value
IGMP Proxy status	Disable
IGMP packet suppression status	Disable
IGMP Querier status	Disable
Source IP address for IGMP Querier and IGMP Proxy to send packets	Use the IP address of IP interface 0. If IP interface 0 is not configured, use 0.0.0.0.
IGMP query interval	60s
Maximum response time to send Query packets	10s
Interval for last member to send Query packets	1s

5.4.3 Configuring IGMP Proxy

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mvr proxy	Enable IGMP Proxy.  Note After global MVR Proxy is enabled, MVR packet suppression and IGMP querier are enabled as well.
3	Alpha-A28E(config)# mvr proxy suppression	Enable IGMP packet suppression. IGMP packet suppression can be enabled or disabled when MVR is enabled.
4	Alpha-A28E(config)# ip igmp querier enable	(Optional) enable IGMP querier. IGMP querier can be enabled or disabled when IGMP Snooping or MVR is enabled.

Step	Configuration	Description
5	Alpha-A28E(config)#mvr proxy source-ip <i>ip-address</i>	(Optional) configure the source IP address for the IGMP querier to send query packets.
6	Alpha-A28E(config)#ip igmp querier query-interval <i>period</i>	(Optional) configure IGMP query interval.
7	Alpha-A28E(config)#mvr proxy query-max-response-time <i>period</i>	(Optional) configure the maximum response time to send query packets.
8	Alpha-A28E(config)#mvr proxy last-member-query <i>period</i>	(Optional) configure the interval for last member to send query packets.



Note

When IGMP Proxy is disabled, the following parameters of MVR Proxy can be configured: source IP address, query interval, maximum response time to send Query packets, and interval for last member to send Query packets. After IGMP Proxy is enabled, these configurations will take effect immediately.

5.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show mvr proxy	Show configurations of IGMP Proxy.
2	Alpha-A28E# show ip igmp querier vlan	Show user VLAN information to be queried.

5.5 Configuring IGMP filtering

5.5.1 Preparing for configurations

Scenario

The different users in the same multicast group receive different multicast requirements and permissions, and allow configuring filtering rules on the switch which connects multicast router and user host so as to restrict multicast users. The maximum number of multicast groups allowed for users to join can be set.

Prerequisite

- Enable MVR.
- Configure multicast VLAN and group address set.
- Configure the source interface and receiving interfaces, and add the related interfaces to the responding VLANs.

5.5.2 Default configurations of IGMP filtering

Function	Default value
Global IGMP filtering	Disable
IGMP filter profile Profile	None
IGMP filter profile action	Refuse
IGMP filtering under interface	No maximum group limitation. The largest group action is drop, and no application filter profile.
IGMP filtering under interface+VLAN	No maximum group limitation. The largest group action is drop, and no application filter profile.

5.5.3 Enabling global IGMP filtering

Enable global IGMP filtering as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode
2	Alpha-A28E(config)# igmp filter	Enable global IGMP filtering



Note

Before configuring IGMP filter profile or the maximum group limitation, use the **igmp filter** command to enable global IGMP filtering.

5.5.4 Configuring IGMP filtering rules

Configure IGMP filter profile as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode
2	Alpha-A28E(config)# ip igmp profile <i>profile-number</i>	Create an IGMP profile, and enter profile configuration mode.
3	Alpha-A28E(config-igmp-profile)# { permit deny }	Configure IGMP profile action.

Step	Configuration	Description
4	Alpha-A28E(config-igmp-profile)# range <i>start-ip-address</i> [<i>end-ip-address</i>]	Configure the IP multicast address or range to be controlled for access.

5.5.5 Applying IGMP filtering rules

Configure IGMP filter profile as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode
2	Alpha-A28E(config)# interface <i>port</i> <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# ip igmp filter <i>profile-number</i>	(Optional) applying IGMP profile filtering rules on the interface. An IGMP profile can be applied to multiple interfaces, but each interface can be configured with only one IGMP profile.
4	Alpha-A28E(config-port)# exit Alpha-A28E(config)# ip igmp filter <i>profile-number</i> vlan <i>vlan-id</i>	(Optional) applying IGMP profile filtering rules in the VLAN.

5.5.6 Configuring the maximum multicast group number

You can add the maximum multicast group number applied to interface or interface+VLAN.

Configuring the maximum multicast group number on the interface

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode
2	Alpha-A28E(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# ip igmp max-groups <i>group-number</i>	Configure the maximum multicast group number allowed on the interface.
4	Alpha-A28E(config-port)# ip igmp max-groups action { deny replace }	(Optional) configure the action when the number of groups exceeds the maximum multicast group number allowed on the interface.

Configuring the maximum multicast group number in the VLAN

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode
2	Alpha-A28E(config)# ip igmp max-group max-group vlan vlan-id	Configure the maximum multicast group number allowed in the VLAN.
3	Alpha-A28E(config)# ip igmp max-group action { deny replace } vlan vlan-id	(Optional) configure the action when the number of groups exceeds the maximum multicast group number allowed in the VLAN.



Note

By default, there is no limit on the multicast group number. The action for the maximum multicast group is **deny**.

5.5.7 Checking configuration

Check configuration result by the following commands.

No.	Item	Description
1	Alpha-A28E# show ip igmp filter [<i>interface-type interface-number vlan [vlan-id]</i>]	Show application information about IGMP filtering.
2	Alpha-A28E# show ip igmp profile [<i>profile-number</i>]	Show configurations of IGMP profile filtering rules.

5.6 Maintenance

Item	Description
Alpha-A28E(config)# clear mvr interface-type [interface-number] statistics	Clear MVR statistics on the interface.

5.7 Configuration examples

5.7.1 Example for configuring IGMP Snooping

Networking requirements

As shown below, Port 1 on the switch is connected with the multicast router; Port 2 and Port 3 connect users. All multicast users belong to the same VLAN 10; you need to configure IGMP Snooping on the switch to receive multicast data with the address 234.5.6.7.

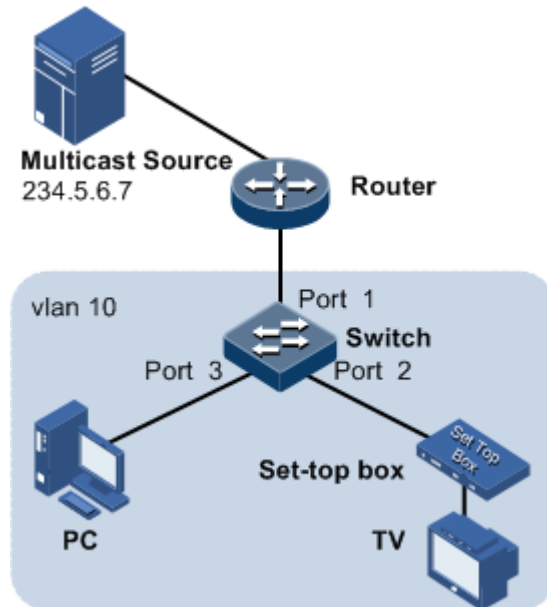


Figure 5-2 IGMP Snooping application networking

Configuration steps

Step 1 Create VLAN and add interface to VLAN.

```
Alpha-A28E#config
Alpha-A28E(config)#create vlan 10 active
Alpha-A28E(config)#interface port 1
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk native vlan 10
Alpha-A28E(config-port)#exit
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#switchport access vlan 10
Alpha-A28E(config-port)#exit
Alpha-A28E(config)#interface port 3
Alpha-A28E(config-port)#switchport access vlan 10
Alpha-A28E(config-port)#exit
```

Step 2 Enable IGMP Snooping.

```
Alpha-A28E(config)#igmp snooping  
Alpha-A28E(config)#igmp snooping vlan-list 10
```

Step 3 Configure the multicast router interface.

```
Alpha-A28E(config)#ip igmp snooping mrouter vlan 1 port 1
```

Checking result

Check whether IGMP Snooping configuration is correct.

```
Alpha-A28E#show ip igmp snooping  
IGMP snooping: Enable  
IGMP querier: Disable  
IGMP snooping aging time: 300s  
IGMP snooping active VLAN: 1-4094  
IGMP snooping immediate-leave active VLAN: --
```

5.7.2 Example for configuring MVR and MVR Proxy

Networking requirements

As shown below, Port 1 of the switch connects with the multicast router, and Port 2 and Port 3 connect with users in different VLANs to receive data from multicast 234.5.6.7 and 225.1.1.1.

Configure MVR on the switch to designate VLAN 3 as a multicast VLAN, and then the multicast data can only be copied one time in the multicast VLAN instead of copying for each user VLAN, thus saving bandwidth.

Enabling MVR Proxy on the switch reduces communication between hosts and the multicast router without implementing multicast functions.

When the PC and set-top box are added into the same multicast group, the switch receives two IGMP Report packets and only sends one of them to the multicast router. The IGMP Query packet sent by multicast will no longer be forwarded downstream, but the switch transmits IGMP Query packet periodically.

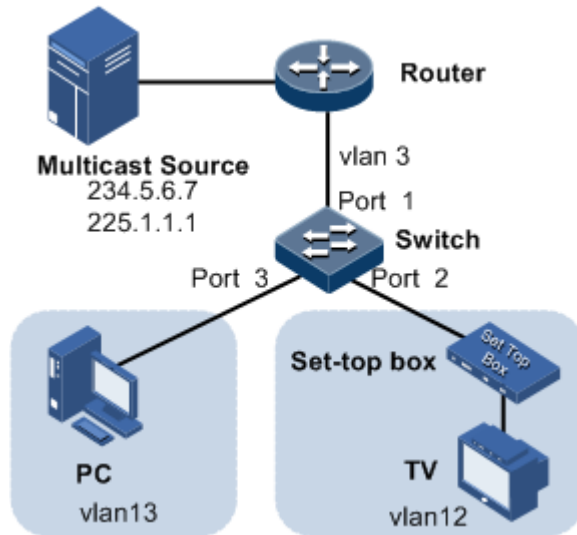


Figure 5-3 MVR application networking

Configuration steps

Step 1 Create VLAN on the switch A and add the interface to it.

```
Alpha-A28E(config)#config
Alpha-A28E(config)#creat vlan 3,12,13 active
Alpha-A28E(config)#interface port 1
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk native vlan 3
Alpha-A28E(config-port)#switchport trunk untagged vlan 12,13
Alpha-A28E(config-port)#exit
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk native vlan 12
Alpha-A28E(config-port)#switchport trunk untagged vlan 3
Alpha-A28E(config-port)#exit
Alpha-A28E(config)#interface port 3
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk native vlan 13
Alpha-A28E(config-port)#switchport trunk untagged vlan 3
```

Step 2 Configure MVR on the switch.

```
Alpha-A28E(config)#mvr enable
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#mvr
Alpha-A28E(config-port)#exit
Alpha-A28E(config)#interface port 3
Alpha-A28E(config-port)#mvr
```

Step 3 Specify the multicast VLAN and group address set.

```
Alpha-A28E(config)#mvr vlan 3
Alpha-A28E(config)#mvr vlan 3 group 234.5.6.7
Alpha-A28E(config)#mvr vlan 3 group 225.1.1.1
```

Step 4 Enable MVR Proxy.

```
Alpha-A28E(config)#mvr proxy
Alpha-A28E(config)#mvr proxy suppression
Alpha-A28E(config)#ip igmp querier enable
Alpha-A28E(config)#mvr proxy source-ip 192.168.1.2
```

Step 5 Configure source interface information.

```
Alpha-A28E(config)#interface port 1
Alpha-A28E(config-port)#mvr type source
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk native vlan 3
Alpha-A28E(config-port)#switchport trunk untagged vlan 12,13
```

Step 6 Configure receiving interface information.

```
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#mvr type receiver
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk native vlan 12
Alpha-A28E(config-port)#switchport trunk untagged vlan 3
Alpha-A28E(config-port)#exit
Alpha-A28E(config)#interface port 3
Alpha-A28E(config-port)#mvr type receiver
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk native vlan 13
Alpha-A28E(config-port)#switchport trunk untagged vlan 3
```

Checking result

Check whether MVR configurations on the switch are correct.

```
Alpha-A28E#show mvr
MVR Running: Enable
MVR Multicast VLAN(ref):3(2)
MVR Max Multicast Groups: 3840
MVR Current Multicast Groups: 2
```

```
MVR Timeout: 600 (second)
MVR Mode: Dynamic
Mvr general query translate vlan: 0
```

Check whether the multicast VLAN and group address information are correct.

```
Alpha-A28E#show mvr vlan group
Vlan Group Address
-----
3     225.1.1.1
3     234.5.6.7
```

Group address entries for all vlans: 2

Check whether IGMP Proxy configurations are correct.

```
Alpha-A28E#show mvr proxy
Mvr Proxy Suppression Status:    Enable
Ip Igmp Querier Status:         Enable
Mvr Proxy Source Ip:            192.168.1.2
Mvr Proxy Version:              v2
Ip Igmp Query Interval(s):      60
Query Response Interval(s):     10
Last Member Query Interval(s):  1
Next IGMP General Query(s):     60
```

5.7.3 Example for applying IGMP filtering and maximum multicast group number to the interface

Networking requirements

Enable IGMP filtering on the switch. Add filtering rules on the interface to filter multicast users.

As shown below,

- Create an IGMP filtering rule Profile 1, set the action to pass for the multicast group ranging from 234.5.6.7 to 234.5.6.10.
- Apply filtering IGMP filtering rule Profile 1 on Port 2, allow the set top box to join the 234.5.6.7 multicast group, forbid it to join the 234.5.6.11 multicast group.
- Apply no filtering rule on Port 3, and allow PCs to join the 234.5.6.11 multicast group.

Configure the maximum multicast group number on Port 2. After the set top box is added to the 234.5.6.7 multicast group, add it to the 234.5.6.8 multicast group. Then, it quits the 234.5.6.7 multicast group.

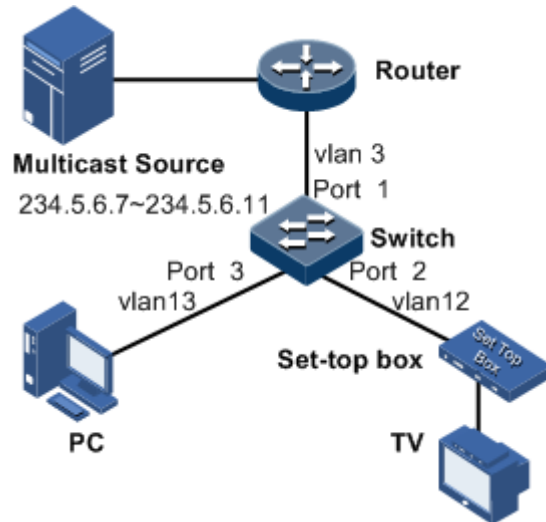


Figure 5-4 Applying IGMP filtering on the interface

Configuration steps

Step 1 Create a VLAN, and create IGMP filtering rules.

```
Alpha-A28E#config
Alpha-A28E(config)#creat vlan 3,12,13 active
Alpha-A28E(config)#ip igmp profile 1
Alpha-A28E(config-igmp-profile)#range 234.5.6.7 234.5.6.10
Alpha-A28E(config-igmp-profile)#permit
```

Step 2 Enable MVR and IGMP filtering.

```
Alpha-A28E(config)#mvr enable
Alpha-A28E(config)#mvr vlan 3
Alpha-A28E(config)#mvr vlan 3 group 234.5.6.7 5
Alpha-A28E(config)#ip igmp filter
```

Step 3 Configure the source interface.

```
Alpha-A28E(config)#interface port 1
Alpha-A28E(config-port)#mvr type source
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk native vlan 3
Alpha-A28E(config-port)#switchport trunk untagged vlan 12,13
```

Step 4 Configure the receiving interface on the set top box, and apply IGMP filtering rule and set the maximum multicast group number.

```
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#mvr type receiver
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk native vlan 12
Alpha-A28E(config-port)#switchport trunk untagged vlan 3
Alpha-A28E(config-port)#ip igmp filter 1
Alpha-A28E(config-port)#ip igmp max-groups 1
Alpha-A28E(config-port)#ip igmp max-groups action replace
```

Step 5 Configure the receiving interface on the PC.

```
Alpha-A28E(config)#interface port 3
Alpha-A28E(config-port)#mvr type receiver
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk native vlan 13
Alpha-A28E(config-port)#switchport trunk untagged vlan 3
```

Checking result

Check whether IGMP filtering is correctly configured on the interface.

```
Alpha-A28E#show ip igmp filter port 2
IGMP Filter: 1
Max Groups: 1
Current groups: 0
Action: Replace
```

5.7.4 Example for applying IGMP filtering and maximum multicast group number to the VLAN

Networking requirements

Enable IGMP filtering on the switch. Add filtering rules in the VLAN to filter multicast users.

As shown below,

- Create an IGMP filtering rule Profile 1, set the action to pass for the multicast group ranging from 234.5.6.7 to 234.5.6.10.
- Apply filtering IGMP filtering rule Profile 1 on VLAN 12, allow the set top box to join the 234.5.6.7 multicast group, forbid it to join the 234.5.6.11 multicast group.
- Apply no filtering rule on VLAN 3, and allow PCs to join the 234.5.6.11 multicast group.

Configure the maximum multicast group number in VLAN 12. After the set top box is added to the 234.5.6.7 multicast group, add it to the 234.5.6.8 multicast group. Then, it quits the 234.5.6.7 multicast group.

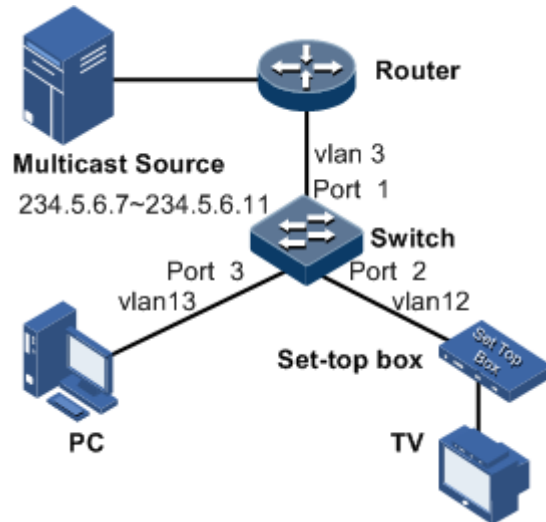


Figure 5-5 Applying IGMP filtering in the VLAN

Configuration steps

Step 1 Create a VLAN, and create IGMP filtering rules.

```
Alpha-A28E#config
Alpha-A28E(config)#creat vlan 3,12,13 active
Alpha-A28E(config)#ip igmp profile 1
Alpha-A28E(config-igmp-profile)#range 234.5.6.7 234.5.6.10
Alpha-A28E(config-igmp-profile)#permit
```

Step 2 Enable MVR and IGMP filtering.

```
Alpha-A28E(config)#mvr enable
Alpha-A28E(config)#mvr vlan 3
Alpha-A28E(config)#mvr vlan 3 group 234.5.6.7 5
Alpha-A28E(config)#ip igmp filter
```

Step 3 Configure the source interface.

```
Alpha-A28E(config)#ip igmp filter 1 vlan 12
Alpha-A28E(config)#ip igmp max-group 1 vlan 12
Alpha-A28E(config)#ip igmp max-group action replace vlan 12
```

Step 4 Configure the receiving interface on the set top box, and apply IGMP filtering rule and set the maximum multicast group number.

```
Alpha-A28E(config)#interface port 1
Alpha-A28E(config-port)#mvr type source
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk native vlan 3
Alpha-A28E(config-port)#switchport trunk untagged vlan 12,13
```

Step 5 Configure the receiving interface on the PC.

```
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#mvr type receiver
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk native vlan 12
Alpha-A28E(config-port)#switchport trunk untagged vlan 3
Alpha-A28E(config-port)#exit
Alpha-A28E(config)#interface port 3
Alpha-A28E(config-port)#mvr type receiver
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk native vlan 13
Alpha-A28E(config-port)#switchport trunk untagged vlan 3
```

Checking result

Check whether IGMP filtering is correctly configured in the VLAN.

```
Alpha-A28E#show ip igmp filter vlan 12
```

VLAN	Filter	Max Groups	Current Groups	Action
12	1	1	0	Replace

6 Security

This chapter introduces basic principle and configuration of security and provides related configuration applications, including the following chapters:

- ACL
- Secure MAC address
- Dynamic ARP inspection
- RADIUS
- TACACS+
- Storm control
- 802.1x
- IP Source Guard
- PPPoE+
- Loopback detection
- Line detection

6.1 ACL

6.1.1 Introduction

Access Control List (ACL) is a set of ordered rules, which can control the A10E/A28E to receive or discard some data packet, thus eliminate impact of invalid packets on the network.

You need to configure rules in network to control illegal packets influent network performance and decide packets allowed passing. These rules are defined by ACL.

ACL is a series of rule composed of permit | deny sentences. The rules are described according to source address, destination address, port ID of data packets. The device judges whether to receive or discard packets according to the rules.

6.1.2 Preparing for configurations

Scenario

ACL can help network device to recognize filter objects. The device recognizes special objects and then permits/denies packets passing according to the configured policy.

ACL includes the below types:

- **IP ACL:** make classifications rule according to source or destination address taken by packets IP head, port ID used by TCP or UDP, and other attributes of packets.
- **MAC ACL:** make classification rule according to source MAC address, destination MAC address, Layer 2 protocol type taken by packets Layer 2 frame head, etc. attributes.
- **MAP ACL:** MAP ACL can define more protocols and more detailed protocol fields than IP ACL and MAC ACL, also can match any bytes of the first 64 bytes according to user's definition.

There are 3 kinds of ACL application according to difference of application environment: ACL based on the whole device, based on interface, and based on VLAN.

Prerequisite

N/A

6.1.3 Default configurations of ACL

The default configuration of ACL is as below.

Function	Default value
Function status of device filter	Disable
Non-fragmenting packet message type	No match
ICMP packet message type	No match
Filter function effective status	Take effect
MAC address matching rules	No match
CoS value matching rules	No match
Ethernet frame type matching rules	No match
ARP protocol type matching rules	No match
ARP packet and MAC/IP address matching rules	No match
IP packet address, DSCP, priority, and matching rule between priority and ToS	No match
Matching rule between port ID and protocol tag bit of TCP packets	No match
Port ID matching rules of UDP packets	No match

Function	Default value
IGMP packet message type matching rules	No match
IPv6 packet matching rules	No match

6.1.4 Configuring IP ACL

Configure IP ACL for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip-access-list <i>acl-id</i> { deny permit } { <i>protocol-id</i> icmp igmp ip } { <i>source-address mask</i> any } { <i>destination-address mask</i> any } Alpha-A28E(config)# ip-access-list <i>acl-number</i> { deny permit } { tcp udp } { <i>source-ip-address ip-mask</i> any } [<i>source-protocol-port</i>] { <i>destination-ip-address ip-mask</i> any } [<i>destination-protocol-port</i>]	Configure IP ACL.
3	Alpha-A28E(config)# interface ip <i>if-number</i> Alpha-A28E(config-ip)# ip ip-access-list { <i>list-number</i> all } [port-list <i>port-list</i>]	Apply ACL on the A10E/A28E.

6.1.5 Configuring MAC ACL

Configure MAC ACL for the A10E/A28E as below.


Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# mac-access-list <i>acl-id</i> { deny permit } [<i>protocol-id</i> arp ip rarp any] { <i>source-mac-address</i> [src-mask <i>src-mask</i>] any } { <i>destination-mac-address</i> [dst-mask <i>dst-mask</i>] any }	Configure MAC ACL.

6.1.6 Configuring MAP ACL

Configure MAP ACL for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# access-list-map <i>acl-id</i> { deny permit }	Create MAP ACL list and enter ACLMAP configuration mode.
3	Alpha-A28E(config-aclmap)# match mac { destination source } <i>mac-address</i>	(Optional) define match rule for source or destination MAC address.
4	Alpha-A28E(config-aclmap)# match cos <i>cos-value</i>	(Optional) define match rule for Cos value.
5	Alpha-A28E(config-aclmap)# match ethertype <i>ethertype</i> [<i>ethertype-mask</i>]	(Optional) define match rule for Ethernet frame type.
6	Alpha-A28E(config-aclmap)# match { arp eapol flowcontrol ip ipv6 loopback mpls mpls-mcast pppoe pppoedisc x25 x75 }	(Optional) define match rule for upper layer protocol type carried by laryer-2 packets head.
7	Alpha-A28E(config-aclmap)# match arp opcode { reply request }	(Optional) define match rule for ARP protocol type (reply packet/request packet).
8	Alpha-A28E(config-aclmap)# match arp { sender-mac target-mac } <i>mac-address</i>	(Optional) define match rule for MAC address of ARP packet.
9	Alpha-A28E(config-aclmap)# match arp { sender-ip target-ip } <i>ip-address</i> [<i>ip-address-mask</i>]	(Optional) define match rule for IP address of ARP packet.
10	Alpha-A28E(config-aclmap)# match ip { destination-address source-address } <i>ip-address</i> [<i>ip-address-mask</i>]	(Optional) define match rule for source or destination IP address.
11	Alpha-A28E(config-aclmap)# match ip precedence { <i>precedence-value</i> critical flash flash-override immediate internet network priority routine }	(Optional) define match rule for IP packet priority.
12	Alpha-A28E(config-aclmap)# match ip tos { <i>tos-value</i> max-reliability max-throughput min-delay min-monetary-cost normal }	(Optional) define match rule for ToS value of IP packet priority.

Step	Configuration	Description
13	Alpha-A28E(config-aclmap)# match ip dscp { <i>dscp-value</i> af11 af12 af13 af21 af22 af23 af31 af32 af33 af41 af42 af43 cs1 cs2 cs3 cs4 cs5 cs6 cs7 default ef }	(Optional) define match rule for DSCP value of IP packet.
14	Alpha-A28E(config-aclmap)# match ip protocol <i>protocol-id</i>	(Optional) define match rule for protocol value of IP packet.
15	Alpha-A28E(config-aclmap)# match ip tcp { destination-port source-port } { <i>port-id</i> bgp domain echo exec finger ftp ftp-data gopher hostname ident irc klogin kshell login lpd nntp pim-auto-rp pop2 pop3 smtp sunrpc syslog tacacs talk telnet time uucp whois www }	(Optional) define match rule for port ID of TCP packet.
16	Alpha-A28E(config-aclmap)# match ip tcp { ack fin psh rst syn urg }	(Optional) define match rule for TCP protocol tag.
17	Alpha-A28E(config-aclmap)# match ip udp { destination-port source-port } { <i>port-id</i> biff bootpc bootps domain echo mobile-ip netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip snmp snmptrap sunrpc syslog tacacs talk tftp time who }	(Optional) Define match rule for port ID of UDP packet.
18	Alpha-A28E(config-aclmap)# match ip icmp <i>icmp-type-id</i> [<i>icmp-code</i>]	(Optional) define match rule for message type of ICMP packet.
19	Alpha-A28E(config-aclmap)# match ip no-fragments	(Optional) define match rules for message type of non-fragment packets.
20	Alpha-A28E(config-aclmap)# match ip igmp { <i>igmp-type-id</i> dvmrp leave-v2 pim-v1 query report-v1 report-v2 report-v3 }	(Optional) define match rule for message type of IGMP packets.

Step	Configuration	Description
21	Alpha-A28E(config- aclmap)# match user-define <i>rule-string rule-mask offset</i>	<p>(Optional) configure match rule for user-defined field, that is, two parameters of rule mask and offset take any byte from bytes 23 to 63 of the first 64 bytes, then comparing with user-defined rule to filter out matched data frame for processing.</p> <p>For example, if you want to filter all TCP packets, you can define:</p> <ul style="list-style-type: none"> • Rule: "06" • Rule mask: "FF" • Offset: "27" <p>The rule mask and offset value work together to filter out content of TCP protocol ID field, then comparing with rule and match with all TCP packets.</p> <p> Note</p> <p>The rule number must be a hex digital. Offset includes field 802.1q VLAN Tag, even though the A10E/A28E receives Untag packets.</p>

6.1.7 Applying ACL

Configure ACL for the A10E/A28E as below.



ACL cannot take effective until it is added into the filter. Multiple ACL match rules can be added into the filter to form multiple filter rules. When configuring filter, the order to add ACL match rule decides priority of the rule. The later the rules are added, the higher the priority is. If the multiple rules are conflicted in matching calculation, take the higher priority rule as standard. Please pay attention to the order of rules when setting the commands so as to filter packets correctly.

Applying ACL to the whole device

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# filter { ip-access-list mac-access-list access-list-map } { <i>acl-list</i> all } [statistics]	Configure filter for the whole device. If the parameter of statistics is configured, the system will statically account according to filter rule.
3	Alpha-A28E(config)# filter enable	Enable filter and the rules. Enable filter cannot only active the filter rules, but also make the filter rules set later become effective.

Applying ACL to the physical interface

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# filter { access-list-map ip-access-list mac-access-list } { all <i>acl-list</i> } ingress interface-type interface-list [statistics]	Configure ACL on the interface. If you configure the parameter statistics , the system takes statistics according to filtering rules.
3	Alpha-A28E(config)# filter access-list-mac { all <i>acl-list</i> } ingress interface-type interface-list valid	(Optional) Enable interface-based filter. Use the filter { access-list-map ip-access-list mac-access-list } { all <i>acl-list</i> } ingress interface-type interface-list invalid command to disable filter function.
4	Alpha-A28E(config)# filter enable	Enable filter and the rules. Enabling filter not only activates the filter rules, but also makes the filter rules set later become effective.

Applying ACL to the VLAN

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# filter { ip-access-list mac-access-list access-list-map } { <i>acl-list</i> all } vlan <i>vlan-id</i> [double-tagging inner] [statistics]	Configure ACL on interface. If you configure the parameter statistics , the system takes statistics according to filtering rules.
3	Alpha-A28E(config)# filter enable	Enable filter and the rules. Enabling filter not only activates the filter rules, but also makes the filter rules set later become effective.

6.1.8 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show ip-access-list [<i>list-number</i>]	Show IP ACL configuration.
2	Alpha-A28E# show mac-access-list [<i>list-number</i>]	Show MAC ACL configuration.
3	Alpha-A28E# show access-list-map [<i>list-number</i>]	Show MAP ACL configuration.
4	Alpha-A28E# show filter [<i>filter-number-list</i>]	Show filter configuration.
5	Alpha-A28E# show interface ip ip-access-list	Show configurations of the filter on the Layer 3 interface.

6.1.9 Maintenance

You can maintain the A10E/A28E as below.

Command	Description
Alpha-A28E(config)# clear filter statistics	Clear filter statistics.

6.2 Secure MAC address

6.2.1 Introduction

Port security MAC is mainly used for the switching device on the edge of the network user side, which can ensure the security of access data on some interfaces, control the input packets according to source MAC address.

You can enable port security MAC to limit and distinguish which users can access the network through secure port. Only packets from the secure MAC addresses can access the network, and unsecure MAC addresses will be dealt with as configured interface access violation mode.

Secure MAC address classification

Secure MAC addresses supported by the device are divided into the following three categories:

- Static secure MAC address

Static secure MAC address is configured by user on secure interface manually; this MAC address will take effect when port security MAC is enabled. Static secure MAC address does not age and supports loading configuration.

- Dynamic secure MAC address

The dynamic secure MAC address is learnt by the device. You can set the learnt MAC address to secure MAC address in the range of the maximum number of learnt MAC address. The dynamic secure MAC addresses ages and does not support configuration load.

Dynamic secure MAC address can be converted to Sticky secure MAC address if needed, so as not to age and support configuration load.

- Sticky secure MAC address

Sticky secure MAC address is generated from the manual configuration of users in secure interface or converted from dynamic secure MAC address. Different from static secure MAC address, Sticky secure MAC address needs to be used in conjunction with Sticky learning:

- When Sticky learning is enabled, Sticky secure MAC address will take effect and this address will not age and support loading configurations.
- When Sticky learning is disabled, Sticky secure MAC address will lose effectiveness and be saved only in the system.



Note

- When Sticky learning is enabled, all dynamic secure MAC addresses learnt from an interface will be converted to Sticky secure MAC addresses.
- When Sticky learning is disabled, all Sticky secure MAC addresses on an interface will be converted to dynamic secure MAC addresses.

Processing mode for violating secure MAC address

When the number of secure MAC addresses has already reached the maximum number, the strange source MAC address packets inputting will be regarded as violation operation. For the illegal user access, there are different processing modes to configure the switch according to secure MAC violation policy:

- Protect mode: for illegal access users, secure interface will discard the user's packets directly.
- Restrict mode: for illegal access users, secure interface will discard the user's packets, and the console will print Syslog information and send alarm to the network management system.
- Shutdown mode: for illegal access users, secure interface will discard the user's packets, and the console will print Syslog information and send alarm to the network management system and then shut down the secure interface.

Caution

When the MAC address is in drift, that is, the secure interface A receives one user access corresponding a secure MAC address on secure interface B, secure interface A will take it as violation processing.

6.2.2 Preparing for configurations

Scenario

In order to ensure the security of data accessed by the interface of the switch, you can control the input packets according to source MAC address. With secure MAC address, you can configure permitting specified users to access the interface, or permitting specified number of users to access from this interface only. However, when the number of users exceeds the limit, the accessed packets will be processed in accordance with secure MAC address violation policies.

Prerequisite

N/A

6.2.3 Default configurations of secure MAC address

The default configuration of port security MAC is as below.

Function	Default value
Interface secure MAC	Disable
Aging time of dynamic secure MAC address	300s
Dynamic secure MAC Sticky learning	Disable
Port secure MAC Trap	Disable
Port secure MAC violation processing mode	Protect
The maximum number of port security MAC	1

6.2.4 Configuring basic functions of secure MAC address

Caution

- We do not suggest that you enable port security MAC on member interfaces of the link aggregation group.
- We do not suggest that you use MAC address management function to configure static MAC addresses when port security MAC is enabled.
- Port security MAC and 802.1x are mutually exclusive. We do not suggest configuring them concurrently.
- Port security MAC and interface-based MAC address number limit are mutually exclusive. We do not suggest configuring them concurrently.

- Port security MAC and MAC address number limit based on interface+VLAN are mutually exclusive. We do not suggest configuring them concurrently.

Configure basic functions of secure MAC address for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# switchport port-security	Enable port security MAC.
4	Alpha-A28E(config-port)# switchport port-security maximum <i>maximum</i>	(Optional) configure the maximum number of secure MAC address.
5	Alpha-A28E(config-port)# switchport port-security violation { protect restrict shutdown }	(Optional) configure secure MAC violation mode.
6	Alpha-A28E(config-port)# no port-security shutdown	(Optional) re-enable the interface which is shut down due to violating the secure MAC address.



Note

When secure MAC violation policy is in Shutdown mode, you can use this command to re-enable this interface which is shut down due to violating secure MAC address. When the interface is Up, the configured secure MAC violation mode will continue to be valid.

6.2.5 Configuring static secure MAC address

Configure static secure MAC address for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# switchport port-security mac-address <i>mac-address</i> vlan <i>vlan-id</i>	Enable static port security MAC.
4	Alpha-A28E(config-port)# switchport port-security	Configure secure MAC address.

6.2.6 Configuring dynamic secure MAC address

Configure dynamic secure MAC address for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# port-security aging-time period	(Optional) configure the aging time of dynamic secure MAC address.
3	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
4	Alpha-A28E(config-port)# switchport port-security	Enable dynamic secure MAC learning.
5	Alpha-A28E(config-port)# switchport port-security trap enable	(Optional) enable port security MAC Trap.




Note

The **switchport port-security** command can enable port security MAC and dynamic secure MAC learning at the same time.

6.2.7 Configuring Sticky secure MAC address

Configure Sticky secure MAC address for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# switchport port-security	(Optional) enable port security MAC.
4	Alpha-A28E(config-port)# switchport port-security mac-address sticky mac-address vlan vlan-id	Manually configure Sticky secure MAC learning.

Step	Configuration	Description
5	Alpha-A28E(config-port)# switchport port-security mac-address sticky	(Optional) manually configure Sticky secure MAC addresses.  Note After Sticky port secure MAC learning is enabled, dynamic security port AMC is translated into the Sticky MAC address. Manually configured Sticky security MAC address takes effect.

6.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show port-security [port-list port-list]	Show interface configurations of port security MAC.
2	Alpha-A28E# show port-security mac-address [port-list port-list]	Show secure MAC address configuration and secure MAC address learning configurations.

6.2.9 Maintenance

Maintain the A10E/A28E as below.

Command	Description
Alpha-A28E(config-port)# clear port-security { all configured dynamic sticky }	Clear a specified secure MAC address type on a specified interface.

6.2.10 Example for configuring secure MAC address

Networking requirements

As shown below, the switch connects 3 user networks. To ensure the security of switch interface access data, the configuration is as below.

- Port 1 permits 3 users to access network at most. The MAC address of one user is specified to 0000.0000.0001. The other 2 users dynamically learn the MAC addresses; the NView NNM system will receive Trap information once the user learns a MAC address. Violation mode is set to Protect and the aging time of the two learned MAC addresses is set 10min.

- Port 2 permits 2 users to access network at most. The 2 user MAC addresses are confirmed through learning; once they are confirmed, they will not age. Violation mode is set to Restrict mode.
- Port 3 permits 1 user to access network at most. The specified user MAC address is 0000.0000.0002. The user MAC address can be controlled whether to age. Violation mode adopts Shutdown mode.

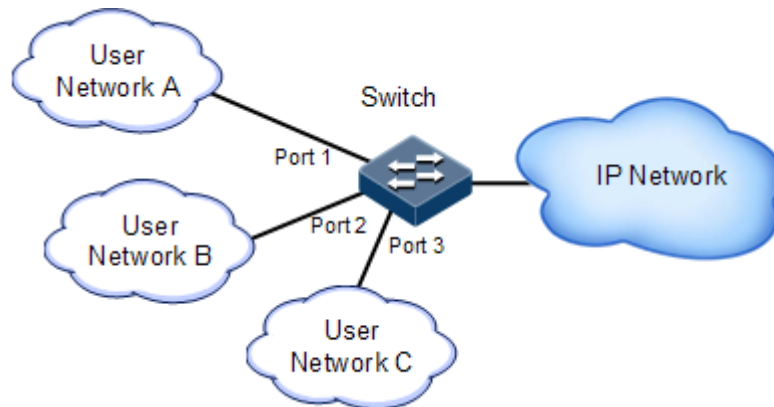


Figure 6-1 Configuring secure MAC address

Configuration steps

Step 1 Configure the secure MAC address of the Port 1.

```
Alpha-A28E#config
Alpha-A28E(config)#interface port 1
Alpha-A28E(config-port)#switchport port-security
Alpha-A28E(config-port)#switchport port-security maximum 3
Alpha-A28E(config-port)#switchport port-security mac-address
0000.0000.0001 vlan 1
Alpha-A28E(config-port)#switchport port-security violation protect
Alpha-A28E(config-port)#switchport port-security trap enable
Alpha-A28E(config-port)#exit
Alpha-A28E(config)#port-security aging-time 10
```

Step 2 Configure the secure MAC address of the Port 2.

```
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#switchport port-security
Alpha-A28E(config-port)#switchport port-security maximum 2
Alpha-A28E(config-port)#switchport port-security mac-address sticky
Alpha-A28E(config-port)#switchport port-security violation restrict
Alpha-A28E(config-port)#exit
```

Step 3 Configure the secure MAC address of the Port 3.

```
Alpha-A28E(config)#interface port 3
Alpha-A28E(config-port)#switchport port-security
Alpha-A28E(config-port)#switchport port-security maximum 1
Alpha-A28E(config-port)#switchport port-security mac-address sticky
0000.0000.0002 vlan 1
Alpha-A28E(config-port)#switchport port-security mac-address sticky
Alpha-A28E(config-port)#switchport port-security violation shutdown
```

Checking results

Check whether port security MAC configuration is correct by the command of **show port-security [port-list port-list]**.

```
Alpha-A28E#show port-security port-list 1-3
Port security aging time:10 (mins)
port status Max-Num Cur-Num His-Num vio-Count vio-action Dynamic-Trap
-----
1 Enable 3 1 0 0 protect Enable
2 Enable 2 0 0 0 restrict Disable
3 Enable 1 1 0 0 shutdown Disable
```

Check secure MAC address and secure MAC address learning configurations on an interface by the command of **show port-security mac-address**.

```
Alpha-A28E#show port-security mac-address
VLAN Security-MAC-Address Flag Port Age(min)
-----
2 0000.0000.0001 static 1 --
2 0000.0000.0002 sticky 3 --
```

6.3 Dynamic ARP inspection

6.3.1 Introduction

Dynamic ARP inspection is used for ARP protection of unsecure interface and prevents from responding ARP packets which do not meet the requirements, thus preventing ARP spoofing attack on the network.

There are 2 modes for dynamic ARP inspection:

- Static binding mode: set the binding relationship manually.
- Dynamic binding mode: in cooperation with the DHCP snooping to generate dynamic binding relationship. When DHCP Snooping entry is changed, the dynamic ARP inspection will also update dynamic binding entry synchronously.

The ARP inspection table, which is used for preventing ARP attacks, consists of DHCP snooping entries and statically configured ARP inspection rules, including IP address, MAC address, and VLAN binding information. In addition, the ARP inspection table associates this information with specific interfaces. Dynamic ARP inspection binding table supports the combination of following entries:

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

Dynamic ARP inspection interfaces are divided into the following two kinds according to trust status:

- Trusted interface: the interface will stop ARP inspection, which means taking no ARP protection on the interface. All ARP packets are allowed to pass.
- Untrusted interface: the interface takes ARP protection. Only ARP packets that match the binding table rules are allowed to pass. Otherwise, they are discarded.

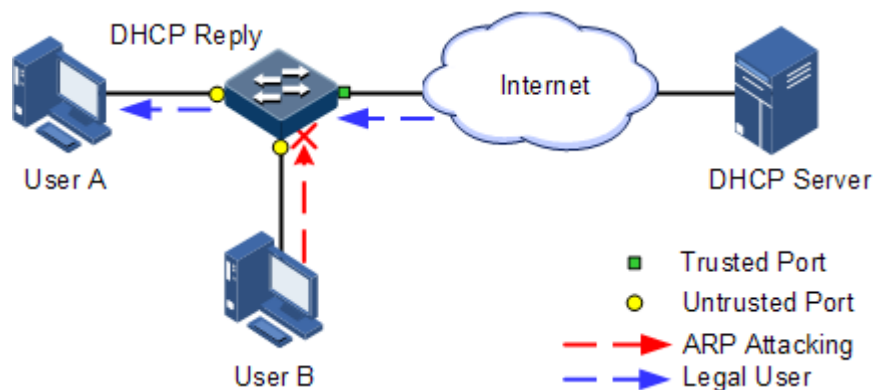


Figure 6-2 Principle of dynamic ARP inspection

Figure 6-2 shows the principle of dynamic ARP inspection. When the A10E/A28E receives an ARP packet, it compares the source IP address, source MAC address, interface ID, and VLAN information of the ARP packet with the DHCP Snooping entry information. If matched, it indicates that it is a legal user and the ARP packets are permitted to pass. Otherwise, it is an ARP attack and the ARP packet is discarded.

Dynamic ARP inspection also provides ARP packet rate limiting to prevent unauthorized users from attacking the device by sending a large number of ARP packets to the A10E/A28E.

- When the number of ARP packets received by an interface every second exceeds the threshold, the system will regard that the interface receives an ARP attack, and then discard all received ARP packets to avoid the attack.
- The system provides auto-recovery and supports configuring the recovery time. The interfaces, where the number of received ARP packets is greater than the threshold, will recover to normal Rx/Tx status automatically after the recovery time expires.

Dynamic ARP inspection can also protect the specified VLAN. After configuring protection VLAN, the ARP packets in specified VLAN on an untrusted interface will be protected. Only the ARP packets, which meet binding table rules, are permitted to pass. Other packets are discarded.

6.3.2 Preparing for configurations

Scenario

Dynamic ARP inspection is used to prevent the common ARP spoofing attacks in the network, which isolates the ARP packets with unsafe sources. Trust status of an interface depends on whether trust ARP packets. However, the binding table decides whether the ARP packets meet requirement.

Prerequisite

Enable DHCP Snooping if there is a DHCP user.

6.3.3 Default configurations of dynamic ARP inspection

The default configuration of dynamic ARP inspection is as below.

Function	Default value
Dynamic ARP inspection interface trust status	Untrusted
Dynamic ARP inspection static binding	Disable
Binding status of dynamic ARP inspection and dynamic DHCP Snooping	Disable
Binding status of dynamic ARP inspection and dynamic DHCP Relay	Disable
Dynamic ARP inspection static binding table	N/A
Dynamic ARP inspection protection VLAN	All VLANs
Interface ARP packets rate limiting	Disable
Interface ARP packets rate limiting	100pps
ARP packets rate limiting recovery	Disable
ARP packets rate limiting recovery time	30s

6.3.4 Configuring trusted interfaces of dynamic ARP inspection

Configure trusted interfaces of dynamic ARP inspection for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# ip arp-inspection trust	Set the interface to a trusted interface.

6.3.5 Configuring static binding of dynamic ARP inspection

Configure static binding of dynamic ARP inspection for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip arp-inspection static-config	Enable global static ARP binding.
3	Alpha-A28E(config)# ip arp-inspection binding ip-address [mac-address] [vlan vlan-id] port port-id	Configure the static binding relationship.

6.3.6 Configuring dynamic binding of dynamic ARP inspection



Caution

Before enabling dynamic binding of dynamic ARP inspection, you need to use the **ip dhcp snooping** command to enable DHCP Snooping.

Configure dynamic binding of dynamic ARP inspection for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip arp-inspection { dhcp-snooping dhcp-relay }	Enable global dynamic ARP binding.

6.3.7 Configuring protection VLAN of dynamic ARP inspection

Configure protection VLAN of dynamic ARP inspection for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip arp-inspection { dhcp-snooping dhcp-relay }	Enable global dynamic ARP binding.
3	Alpha-A28E(config)# ip arp-inspection vlan vlan-list	Configure protection VLAN of dynamic ARP inspection.

6.3.8 Configuring rate limiting on ARP packets on the interface

Configure rate limiting on ARP packets on the interface for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# ip arp-rate-limit enable	Enable interface ARP packet rate limiting.
4	Alpha-A28E(config-port)# ip arp-rate-limit rate rate-value	Configure rate limiting on ARP packets on the interface.

6.3.9 Configuring global ARP packet rate limiting auto-recovery time

Configure ARP packet rate limiting auto-recovery time for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip arp-rate-limit recover enable	Enable ARP packet rate limiting auto-recovery.
3	Alpha-A28E(config)# ip arp-rate-limit recover time time	Configure ARP packet rate limiting auto-recovery time.

6.3.10 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show ip arp-inspection	Show dynamic ARP inspection configurations.
2	Alpha-A28E# show ip arp-inspection binding [port port-id]	Show dynamic ARP inspection binding table information.
3	Alpha-A28E# show ip arp-rate-limit	Show ARP packet rate limiting configurations.

6.3.11 Example for configuring dynamic ARP inspection

Networking requirements

To prevent ARP attacks, you need to configure dynamic ARP inspection function on Switch A, as shown in Figure 6-3.

- Uplink Port 3 permits all ARP packets to pass.
- Downlink Port 1 permits ARP packets with specified IP address 10.10.10.1 to pass.
- Other interfaces permit ARP packets complying with dynamic binding learnt by DHCP snooping to pass.
- Downlink Port 2 configures ARP packets rate limiting. The rate threshold is set to 20 pps and rate limiting recovery time is set to 15s.

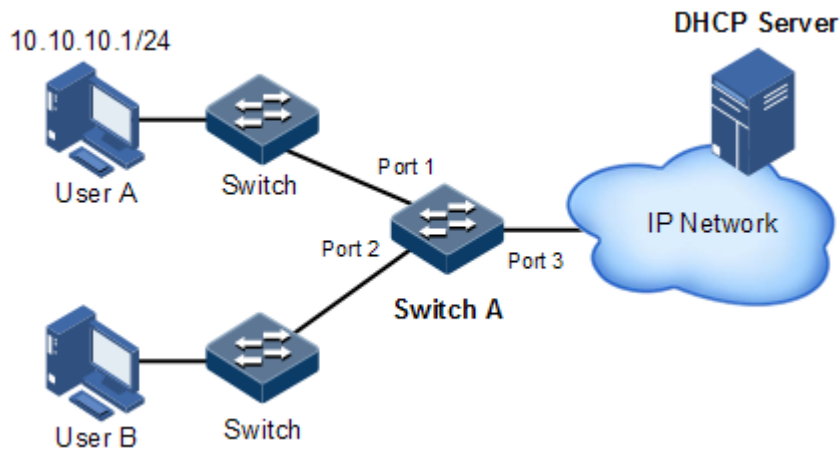


Figure 6-3 Configuring dynamic ARP inspection

Configuration steps

Step 1 Set Port 3 to the trusted interface.

```
Alpha-A28E#config  
Alpha-A28E(config)#interface port 3  
Alpha-A28E(config-port)#ip arp-inspection trust  
Alpha-A28E(config-port)#exit
```

Step 2 Configure the static binding relationship.

```
Alpha-A28E(config)#ip arp-inspection static-config  
Alpha-A28E(config)#ip arp-inspection binding 10.10.10.1 port 1
```

Step 3 Enable binding between dynamic ARP inspection and dynamic DHCP Snooping.

```
Alpha-A28E(config)#ip dhcp snooping  
Alpha-A28E(config)#ip arp-inspection dhcp-snooping
```

Step 4 Configure ARP packet rate limiting on an interface.


```
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#ip arp-rate-limit rate 20
Alpha-A28E(config-port)#ip arp-rate-limit enable
Alpha-A28E(config-port)#exit
```

Step 5 Configure ARP packet rate limiting auto-recovery.

```
Alpha-A28E(config)#ip arp-rate-limit recover time 15
Alpha-A28E(config)#ip arp-rate-limit recover enable
```

Checking results

Show interface trust status configurations and static/dynamic ARP binding configurations by the command of **show ip arp-inspection**.

```
Alpha-A28E#show ip arp-inspection
Static Config ARP Inspection: Enable
DHCP Snooping ARP Inspection: Enable
DHCP Relay ARP Inspection: Disable
ARP Inspection Protect Vlan : 1-4094
Bind Rule Num           : 1
Vlan Acl Num            : 0
Remained Acl Num        : 512
Port   Trust
-----
1      no
2      no
3      yes
4      no
...
```

Show dynamic ARP binding table information by the command of **show ip arp-inspection binding**.

```
Alpha-A28E#show ip arp-inspection binding
Ip Address      Mac Address  VLAN  Port  Type      Inhw
-----
10.10.10.1     --          --    1     static    yes
Current Rules Num: 1
History Max Rules Num: 1
```

Show interface rate limiting configurations and rate limiting auto-recovery time configurations by the command of **show ip arp-rate-limit**.

```
Alpha-A28E#show ip arp-rate-limit
arp rate limit auto recover: enable
```

```
arp rate limit auto recover time: 15 second
Port   Enable-Status   Rate(Num/Sec)   Overload
-----
1      Disabled        100              No
2      Enabled         20               No
3      Disabled        100              No
4      Disabled        100              No
...
```

6.4 RADIUS

6.4.1 Introduction

Remote Authentication Dial In User Service (RADIUS) is a standard communication protocol that authenticates remote access users intensively. RADIUS uses UDP as the transmission protocol (port 1812 and port 1813) which has a good instantaneity; at the same time, RADIUS supports retransmission mechanism and standby server mechanism which has a good reliability.

RADIUS authentication function

RADIUS adopts client/server mode, network access device is used as client of RADIUS server. RADIUS server receives user connecting requests and authenticates users, then reply configuration information to all clients for providing services. Control user access device and network and improve network security.

Communication between client and RADIUS server is authenticated by sharing key, which will not be transmitted on network. Besides, all user directions need to be encrypted when transmitting between client device and RADIUS server to ensure security.

RADIUS accounting function

RADIUS accounting function is used to authenticate user through RADIUS. User sends a starting account packets to RADIUS accounting server when log in, according to the accounting policy to send update packet to RADIUS server; when log off, send stopping account packet to RADIUS accounting server, the packet includes user online time. RADIUS accounting server can record the access time and operations for each user by the packets.

6.4.2 Preparing for configurations

Scenario

You can deploy RADIUS server in network to take authentication and accounting so as to control user access to device and network. This device can be used as agent of RADIUS server, which authorizes user accessing according to feedback from RADIUS.

Prerequisite

N/A

6.4.3 Default configurations of RADIUS

The default configuration of RADIUS is as below.

Function	Default value
RADIUS accounting	Disable
IP address of RADIUS server	0.0.0.0
IP address of RADIUS accounting server	0.0.0.0
Port ID of RADIUS authentication server	1812
Port ID of RADIUS accounting server	1813
Shared key used for communication with RADIUS accounting server	N/A
Accounting failure processing policy	online
Period for sending update packet	0

6.4.4 Configuring RADIUS authentication


Configure RADIUS authentication for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface ip <i>if-number</i>	Enter Layer 3 interface configuration mode.
3	Alpha-A28E(config-if)# ip address <i>ip-address</i> [<i>ip-</i> <i>mask</i>] [<i>vlan-list</i>]	Configure an IPv4 address.
4	Alpha-A28E(config-if)# end	Return to privileged EXEC mode.
5	Alpha-A28E# radius [backup] <i>ip-address</i> [auth-port <i>port-</i> <i>number</i>]	Assign IP address and port ID for RADIUS authentication server. Configure the backup parameter to assign the backup RADIUS authentication server.
6	Alpha-A28E# radius-key <i>string</i>	Configure the shared key for RADIUS authentication.
7	Alpha-A28E# user login { local-radius local-user radius-local [server-no- response] radius-user }	Configure users performing login authentication through RADIUS.
8	Alpha-A28E# enable login { local-radius local-user radius-local [server-no- response] radius-user }	Set the authentication mode for user entering privileged EXEC mode to RADIUS.

6.4.5 Configuring RADIUS accounting

Configure RADIUS accounting for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface ip <i>if-number</i>	Enter Layer 3 interface configuration mode.
3	Alpha-A28E(config-ip)# ip address ip-address [sub] [<i>ip-mask</i>] [<i>vlan-list</i>]	Configure an IPv4 address.
4	Alpha-A28E(config-ip)# end	Return to privileged EXEC mode.
5	Alpha-A28E# aaa accounting login enable	Enable RADIUS accounting.
6	Alpha-A28E# radius [backup] accounting- server ip-address [<i>account-port</i>]	Assign IP address and UDP port ID for RADIUS accounting server.
7	Alpha-A28E# radius accounting-server key <i>string</i>	Configure the shared key to communicate with the RADIUS accounting server. The shared key must be identical to the one configured on the RADIUS accounting server. Otherwise, accounting fails.
8	Alpha-A28E# aaa accounting fail { offline online }	Configure the processing policy for accounting failure.
9	Alpha-A28E# aaa accounting update period	Configure the period for sending accounting update packets. If configured as 0, no accounting update packet is sent.



Note

The RADIUS accounting server can record access time and operation for each user through accounting starting packets, update packets and accounting end packets.

6.4.6 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show radius-server	Show configurations on the RADIUS server.
2	Alpha-A28E# show aaa accounting	Show configurations of global accounting.

6.4.7 Example for configuring RADIUS

Networking requirements

As shown in Figure 6-4, you need to configure RADIUS authentication and accounting on switch A to authenticate login users and record their operations. The period for sending update packets is 2 set to minutes. The user will be offline if the accounting fails.

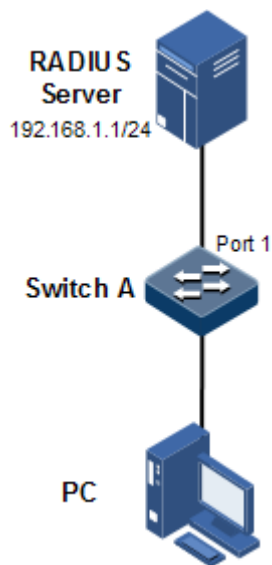


Figure 6-4 Configuring RADIUS

Configuration steps

Step 1 Authenticate login users through RADIUS.

```
Alpha-A28E#radius 192.168.1.1
Alpha-A28E#radius-key alpha-a28e
Alpha-A28E#user login radius-user
Alpha-A28E#enable login local-radius
```

Step 2 Account login users through RADIUS.

```
Alpha-A28E#aaa accounting login enable
Alpha-A28E#radius accounting-server 192.168.1.1
Alpha-A28E#radius accounting-server key alpha-a28e
Alpha-A28E#aaa accounting fail offline
Alpha-A28E#aaa accounting update 2
```

Checking results

Use the **show radius-server** command to check whether the RADIUS server is correctly configured.

```
Alpha-A28E#show radius-server
Authentication server IP:      192.168.1.1 port:1812
Backup authentication server IP:0.0.0.0 port:1812
Authentication server key:    alpha-a28e
Accounting server IP:         192.168.1.1 port:1813
Backup accounting server IP:   0.0.0.0 port:1813
Accounting server key:        alpha-a28e
```

Use the **show aaa accounting** command to check whether the RADIUS accounting is correctly configured.

```
Alpha-A28E#show aaa accounting
Accounting login:              enable
Accounting update interval:    2
Accounting fail policy:        offline
```

6.5 TACACS+

6.5.1 Introduction

Terminal Access Controller Access Control System (TACACS+) is a kind of network access authentication protocol similar to RADIUS. The differences between them are:

- TACACS+ uses TCP port 49, which has higher transmission reliability compared with UDP port used by RADIUS.
- TACACS+ encrypts the holistic of packets except the standard head of TACACS+, and there is an area to show whether the data packets are encrypted in the head of packet. Compared to RADIUS user password encryption, the TACACS+ is much safer.
- TACACS+ authentication function is separated from authorization and accounting functions; it is more flexible in deployment.

In a word, TACACS+ is safer and more reliable than RADIUS. However, as an open protocol, RADIUS is more widely-used.

6.5.2 Preparing for configurations

Scenario

To control users accessing to the A10E/A28E and the network, you can authenticate and account users by deploying the TACACS+ server in the network. Compared with RADIUS,

TACACS+ is safer and more reliable. The A10E/A28E can be used as the agent of the TACACS+ server, controlling users according to feedback result from the TACACS+ server.

Prerequisite

N/A

6.5.3 Default configurations of TACACS+

The default configuration of TACACS+ is as below.

Function	Default value
TACACS+ function	Disable
Login mode	local-user
IP address of TACACS+ authentication server	0.0.0.0, shown as "--"
IP address of TACACS+ accounting server	0.0.0.0, shown as "--"
Shared key used for communication with TACACS+ accounting server	Null
Accounting failure processing policy	online
Period for sending update packet	0

6.5.4 Configuring TACACS+ authentication

Configure TACACS+ authentication for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface ip if-number	Enter Layer 3 interface configuration mode.
3	Alpha-A28E(config-ip)# ip address ip-address [ip-mask] [vlan-list]	Configure an IPv4 address.
4	Alpha-A28E(config-ip)# end	Return to privileged EXEC mode.
5	Alpha-A28E# tacacs-server [backup] ip-address	Assign IP address and port ID for TACACS+ authentication server. Configure the backup parameter to assign the backup TACACS+ authentication server.
6	Alpha-A28E# tacacs-server key string	Configure the shared key for TACACS+ authentication.

Step	Configuration	Description
7	Alpha-A28E# user login { local-tacacs local-user tacacs-local [server-no-response] tacacs-user }	Configure users performing login authentication through TACACS+.
8	Alpha-A28E# enable login { local-tacacs local-user tacacs-local [server-no-response] tacacs-user }	Set the authentication mode for user entering privileged EXEC mode to TACACS+.

6.5.5 Configuring TACACS+ accounting

Configure TACACS+ accounting for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface ip <i>if-number</i>	Enter Layer 3 interface configuration mode.
3	Alpha-A28E(config-ip)# ip address <i>ip-address</i> [<i>ip-mask</i>] [<i>vlan-list</i>]	Configure an IPv4 address.
4	Alpha-A28E(config-ip)# end	Return to privileged EXEC mode.
5	Alpha-A28E# aaa accounting login enable	Enable TACACS+ accounting.
6	Alpha-A28E# tacacs [backup] accounting- server <i>ip-address</i>	Assign IP address and UDP port ID for TACACS+ accounting server.
7	Alpha-A28E# tacacs-server key <i>string</i>	Configure the shared key to communicate with the TACACS+ accounting server.
8	Alpha-A28E# aaa accounting fail { offline online }	Configure the processing policy for accounting failure.
9	Alpha-A28E# aaa accounting update <i>period</i>	Configure the period for sending accounting update packets. If configured as 0, no accounting update packet is sent.


6.5.6 Configuring TACACS+ authorization

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# tacacs authorization enable	Enable TACACS+ authorization server.

6.5.7 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show tacacs-server	Show configurations on the TACACS+ authentication server.
2	Alpha-A28E# show radius-server	Show configurations on the TACACS+ accounting server.  Note The show radius-server command is used to show TACACS+ and RADIUS accounting configurations. By default, the results are RADIUS authentication configurations.

6.5.8 Maintenance

Maintain the A10E/A28E as below.

Command	Description
Alpha-A28E# clear tacacs statistics	Clear TACACS+ statistics.

6.5.9 Example for configuring TACACS+

Networking requirements

As shown in Figure 6-5, you need to configure TACACS+ authentication on Switch A to authenticate users who log in to the A10E/A28E.

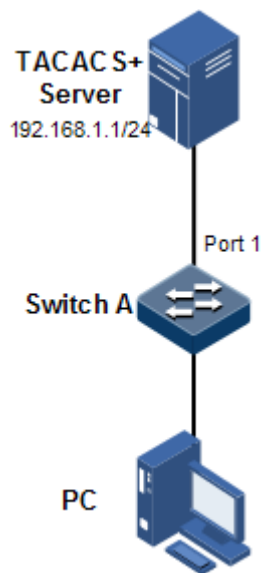


Figure 6-5 Configuring TACACS+

Configuration steps

Authenticate login users through TACACS+.

```
Alpha-A28E#tacacs-server 192.168.1.1
Alpha-A28E#tacacs-server key alpha-a28e
Alpha-A28E#user login tacacs-user
Alpha-A28E#enable login local-tacacs
```

Checking results

Show TACACS+ configurations by the command of **show tacacs-server**.

```
Alpha-A28E#show tacacs-server
Server Address:      192.168.1.1
Backup Server Address:  --
Sever Shared Key:   alpha-a28e
Total Packet Sent:  0
Total Packet Recv:  0
Accounting server Address:  --
Backup Accounting server Address:  --
```

6.6 Storm control

In most Layer 2 network, the unicast traffic is much larger than the broadcast traffic. If rate for broadcast traffic is not limited, when a broadcast storm is generated, a number of

bandwidth will be occupied. Therefore, network performance is reduced and unicast packet cannot be forwarded. In addition, the communication between devices may be interrupted.

Configuring storm control on Layer 2 devices can prevent broadcast storm occurring when broadcast packets increase sharply in the network. And therefore, ensure the unicast packets can be properly forwarded.

After storm control is enabled, the interface will automatically discard the received packets. If storm control is disabled or if the number of received broadcast packets does not reach the pre-configured threshold, the broadcast packets are broadcasted to other interfaces of the switch properly.

6.6.1 Preparing for configurations

Scenario

Configuring storm control in the Layer 2 network can prevent broadcast storm occurring when broadcast packets increase sharply in the network. And therefore, ensure the unicast packets can be properly forwarded.

Broadcast traffic may exist in following forms, so you need to limit the bandwidth for them on Layer 2 devices.

- Unknown unicast traffic: the unicast traffic whose MAC destination address is not in MAC address table. It is broadcasted by Layer 2 devices.
- Unknown multicast traffic: the multicast traffic whose MAC destination address is not in MAC address table. Generally, it is broadcasted by Layer 2 devices.
- Broadcast traffic: the traffic whose MAC destination address is a broadcast MAC address. It is broadcasted by Layer 2 devices.

Prerequisite

Connect the interface properly, and configure it to make it physically Up.

6.6.2 Default configurations of storm control

The default configuration of storm control is as below.

Function	Default value
Broadcast storm control status	Enable
Multicast and unknown unicast storm control status	Disable
Allowed bytes per second	64 Kbit/s
DLF packet forwarding	Enable

6.6.3 Configuring storm control

Configure storm control for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# storm-control { all broadcast d1f multicast } enable port-list <i>port-list</i>	Enable storm control on broadcast traffic, multicast traffic and unknown unicast traffic.
3	Alpha-A28E(config)# storm-control bps <i>value</i>	(Optional) configure the number of bytes that are allowed to pass every second.

6.6.4 Configuring DLF packet forwarding

Configure DLF packet forwarding for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# d1f-forwarding enable	Enable DLF packet forwarding on the interface.

6.6.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show storm-control [<i>interface-type interface-number</i>]	Show configurations of storm control.
2	Alpha-A28E# show d1f-forwarding	Show DLF packet forwarding status.

6.6.6 Example for configuring storm control

Networking requirements

As shown in Figure 6-6, to restrict influence on Switch A caused by broadcast storm, you need to configure storm control on Switch A to control broadcast packets and unknown unicast packets. The control threshold is set to 640 Kbit/s, and burst is set to 80 KBytes.

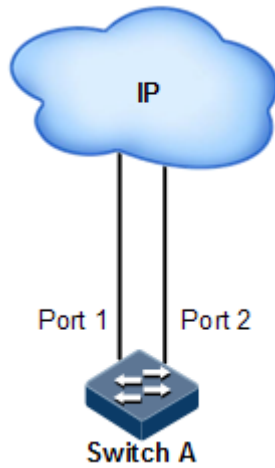


Figure 6-6 Configuring storm control

Configuration steps

Step 1 Configure storm control on Switch A.

```
Alpha-A28E#config
Alpha-A28E(config)#storm-control broadcast enable port 1-2
Alpha-A28E(config)#storm-control dlf enable port 1-2
Alpha-A28E(config)#storm-control bps 640 80
```

Checking results

Show storm control configurations by the command of **show storm-control**.

```
Alpha-A28E#show storm-control
Threshold: 640 kbps
Burst: 80 kB
Port  Broadcast      Multicast      DLF_Unicast
-----
1       Enable           Disable        Enable
2       Enable           Disable        Enable
3       Enable           Disable        Disable
```

6.7 802.1x

6.7.1 Introduction

802.1x, based on IEEE 802.1x, is a VLAN-based network access control technology. It is mainly used to solve authentication and security problems of LAN users.

It is used to authenticate and control access devices at the physical layer of the network device. It defines a point-to-point connection mode between the device interface and user devices. User devices, connected to the interface, can access resources in the LAN if they are authenticated. Otherwise, they cannot access resources in the LAN through the switch.

802.1x structure

As shown in Figure 6-7, 802.1x authentication uses C/S mode, including the following 3 parts:

- **Supplicant:** a user-side device installed with the 802.1x client software (such as Windows XP 802.1x client), such as a PC
- **Authenticator:** an access control device supporting 802.1x authentication, such as a switch
- **Authentication Server:** a device used for authenticating, authorizing, and accounting users. In general, the RADIUS server is taken as the 802.1x authentication server.

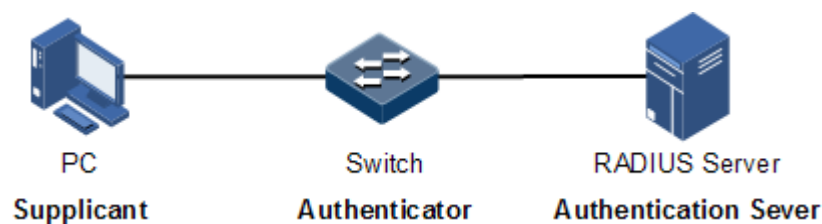


Figure 6-7 802.1x structure

Interface access control modes

The authenticator uses the authentication server to authenticate clients that need to access the LAN and controls interface authorized/ unauthorized status through the authentication results. You can control the access status of an interface by configuring access control modes on the interface. 802.1x authentication supports the following 3 interface access control modes:

- **Protocol authorized mode (auto):** the protocol state machine decides the authorization and authentication results. Before clients are successfully authenticated, only EAPoL packets are allowed to be received and sent. Users are disallowed to access network resources and services provided by the switch. If clients are authorized, the interface is switched to the authorized state, allowing users to access network resources and services provided by the switch.
- **Force interface authorized mode (authorized-force):** the interface is in authorized state, allowing users to access network resources and services provided by the switch without being authorized and authenticated.
- **Force interface unauthorized mode (unauthorized-force):** the interface is in unauthorized mode. Users are disallowed to access network resources and services provided by the switch, that is, users are disallowed to be authenticated.

802.1x authentication procedure

The supplicant and the authentication server exchange information through the Extensible Authentication Protocol (EAP) packet while the supplicant and the authenticator exchange information through the EAP over LAN (EAPoL) packet. The EAP packet is encapsulated with authentication data. This authentication data will be encapsulated into the RADIUS protocol packet to be transmitted to the authentication server through a complex network.

Both the authenticator and the supplicant can initiate the 802.1x authentication procedure. This guide takes the supplicant for an example, as shown below:

- Step 1 The user enters the user name and password. The supplicant sends an EAPoL-Start packet to the authenticator to start the 802.1x authentication.
- Step 2 The authenticator sends an EAP-Request/Identity to the supplicant, asking the user name of the supplicant.
- Step 3 The supplicant replies an EAP-Response/Identity packet to the authenticator, which includes the user name.
- Step 4 The authenticator encapsulates the EAP-Response/Identity packet to the RADIUS protocol packet and sends the RADIUS protocol packet to the authentication server.
- Step 5 The authentication server compares with received encrypted password with the one generated by itself.

If identical, the authenticator modifies the interface state to authorized state, allowing users to access the network through the interface and sends an EAP-Success packet to the supplicant. Otherwise, the interface is in unauthorized state and sends an EAP-Failure packet to the supplicant.

802.1x timers

During 802.1x authentication, the following 5 timers are involved:

- Reauth-period: re-authorization timer. After the period is exceeded, the A10E/A28E re-initiates authorization.
- Quiet-period: quiet timer. When user authorization fails, the A10E/A28E needs to keep quiet for a period. After the period is exceeded, the A10E/A28E re-initiates authorization. During the quiet time, the A10E/A28E does not process authorization packets.
- Tx-period: transmission timeout timer. When the A10E/A28E sends a Request/Identity packet to users, the A10E/A28E will initiate the timer. If users do not send an authorization response packet during the tx-period, the A10E/A28E will re-send an authorization request packet. The A10E/A28E sends this packet three times in total.
- Supp-timeout: Supplicant authorization timeout timer. When the A10E/A28E sends a Request/Challenge packet to users, the A10E/A28E will initiate supp-timeout timer. If users do not send an authorization response packet during the supp-timeout, the A10E/A28E will re-send the Request/Challenge packet. The A10E/A28E sends this packet twice in total.
- Server-timeout: Authentication server timeout timer. The timer defines the total timeout period of sessions between authorizer and the RADIUS server. When the configured time is exceeded, the authenticator will end the session with RADIUS server and start a new authorization process.

6.7.2 Preparing for configurations

Scenario

To realize access authentication on LAN users and ensure access user security, you need to configure 802.1x authentication on the A10E/A28E.

If users are authenticated, they are allowed to access network resources. Otherwise, they cannot access network resources. By performing authentication control on user access interface, you can manage the users.

Prerequisite

If RADIUS authentication server is used, you need to perform following operations before configuring 802.1x authentication:

- Configure the IP address of the RADIUS server and the RADIUS shared key.
- The A10E/A28E can ping RADIUS server successfully.

6.7.3 Default configurations of 802.1x

The default configuration of 802.1x is as below.

Function	Default value
Global 802.1x	Disable
Interface 802.1x	Disable
Interface access control mode	Auto
802.1x authentication method	chap
Interface access control mode of 802.1x authentication	portbase
RADIUS server timeout timer time	100s
802.1x re-authentication	Disable
802.1x re-authentication timer	3600s
802.1x quiet timer time	60s
Request packet retransmission timer timeout	30s
Supplicant authorization timer timeout	30s

6.7.4 Configuring basic functions of 802.1x



Caution

- 802.1x and STP are exclusive on the same interface. You cannot enable them concurrently.
- Only one user authentication request is processed on an interface at a time.

Configure basic functions of 802.1x for the A10E/A28E as below.

Step	Configuration	Description
1	A1pha-A28E# config	Enter global configuration mode.
2	A1pha-A28E(config)# dot1x enable	Enable global 802.1x.

Step	Configuration	Description
3	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
4	Alpha-A28E(config-port)# dot1x authentication-method { chap eap pap }	Configure 802.1x protocol authentication mode.
5	Alpha-A28E(config-port)# dot1x enable	Enable interface 802.1x.
6	Alpha-A28E(config-port)# dot1x auth-control { auto authorized-force unauthorized-force }	Configure interface access control mode.
7	Alpha-A28E(config-port)# dot1x auth-method { macbased portbased }	Configure interface access control mode of 802.1x authentication.



Note

To configure EAP relay authentication mode, ensure that the RADIUS server supports EAP attributes.
If 802.1x is disabled in global/interface configuration mode, the interface access control mode of 802.1x is set to force interface authorized mode.

6.7.5 Configuring 802.1x re-authentication

Configure 802.1x re-authentication for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# dot1x reauthentication enable	Enable 802.1x re-authentication.



Caution

Re-authentication is initiated for authorized users. Before enabling re-authentication, you must ensure that global/interface 802.1x is enabled. Authorized interfaces are still in this mode during re-authentication. If re-authentication fails, the interfaces are in unauthorized state.

6.7.6 Configuring 802.1x timers

Configure 802.1x timers for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# dot1x timer reauth-period reauth-period	Configure the time of the re-authentication timer.
4	Alpha-A28E(config-port)# dot1x timer quiet-period quiet-period	Configure the time of the quiet timer.
5	Alpha-A28E(config-port)# dot1x timer tx-period tx-period	Configure the time of the transmission timeout timer.
6	Alpha-A28E(config-port)# dot1x timer supp-timeout supp-timeout	Configure the time of the supplicant authorization timeout timer.
7	Alpha-A28E(config-port)# dot1x timer server-timeout server-timeout	Configure the time of the Authentication server timeout timer.

6.7.7 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show dot1x port-list port-list	Show interface 802.1x configurations.
2	Alpha-A28E# show dot1x port-list port-list statistics	Show interface 802.1x statistics.
3	Alpha-A28E# show dot1x port-list port-list user	Show user information of interface 802.1x authentication.

6.7.8 Maintenance

Maintain the A10E/A28E as below.

Command	Description
Alpha-A28E(config)# clear dot1x port-list port-list statistics	Clear interface 802.1x statistics.

6.7.9 Example for configuring 802.1x

Networking requirements

To make users access external network, you need to configure 802.1x authentication on the switch, as shown in Figure 6-8.

- Configure the switch.
 - IP address: 10.10.0.1
 - Subnet mask: 255.255.0.0
 - Default gateway address: 10.10.0.2
- Perform authorization and authentication through the RADIUS server.
 - IP address of the RADIUS server: 192.168.0.1
 - Password of the RADIUS server: alpha-a28e
- Set the interface access control mode to protocol authorized mode.
- After authorized successfully, the user can initiate re-authentication in 600 seconds.

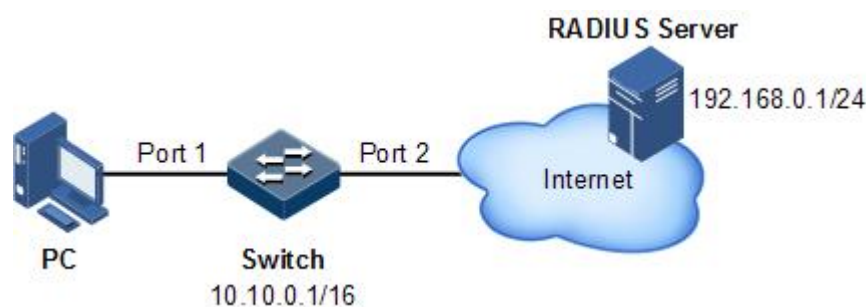


Figure 6-8 Configuring 802.1x

Configuration steps

Step 1 Configure the IP addresses of the switch and RADIUS server.

```
Alpha-A28E#config
Alpha-A28E(config)#interface ip 0
Alpha-A28E(config-ip)#ip address 10.10.0.1 255.255.0.0 1
Alpha-A28E(config-ip)#exit
Alpha-A28E(config)#ip default-gateway 10.10.0.2
Alpha-A28E(config)#exit
Alpha-A28E#radius 192.168.0.1
Alpha-A28E#radius-key alpha-a28e
```

Step 2 Enable global 802.1x and interface 802.1x.

```
Alpha-A28E#config
Alpha-A28E(config)#dot1x enable
Alpha-A28E(config)#interface port 1
```

```
Alpha-A28E(config-port)#dot1x enable
```

Step 3 Set the authorization mode to protocol authorization mode.

```
Alpha-A28E(config-port)#dot1x auth-control auto
```

Step 4 Enable re-authentication and set the re-authentication time to 600s.

```
Alpha-A28E(config-port)#dot1x reauthentication enable  
Alpha-A28E(config-port)#dot1x timer reauth-period 600
```

Checking results

Show 802.1x configurations by the command of **show dot1x port-list** *port-list*.

```
Alpha-A28E#show dot1x port-list 1  
802.1x Global Admin State: Enable  
802.1x Authentication Method: Chap  
Port 1  
-----  
802.1X Port Admin State:      Enable  
PAE:                          Authenticator  
PortMethod:                   Portbased  
PortControl:                  Auto  
PortStatus:                   Authorized  
Authenticator PAE State:      Initialize  
Backend Authenticator State:  Initialize  
ReAuthentication:            Disable  
QuietPeriod:                  60(s)  
ServerTimeout:               100(s)  
SuppTimeout:                 30(s)  
ReAuthPeriod:                3600(s)  
TxPeriod:                    30(s)
```

6.8 IP Source Guard

6.8.1 Introduction

IP Source Guard uses a binding table to defend against IP Source spoofing and solve IP address embezzlement without identity authentication. IP Source Guard can cooperate with DHCP snooping to generate dynamic binding relationship. In addition, you can configure static binding relationship manually. DHCP Snooping filters untrusted DHCP packets by establishing and maintaining the DHCP binding database.

IP Source Guard binding entry

IP Source Guard is used to match packet characteristics, including source IP address, source MAC address, and VLAN tags, and can support the interface to combine with the following characteristics (hereinafter referred to as binding entries):

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

According to the generation mode of binding entries, IP Source Guard can be divided into static binding and dynamic binding:

- Static binding: configure binding information manually and generate binding entry to complete the interface control, which fits for the case where the number of hosts is small or where you need to perform separate binding on a single host.
- Dynamic binding: obtain binding information automatically from DHCP Snooping to complete the interface control, which fits for the case where there are many hosts and you need to adopt DHCP to perform dynamic host configurations. Dynamic binding can effectively prevent IP address conflict and embezzlement.

IP Source Guard principle

The basic principle of IP Source Guard is to build an IP source binding table within the A10E/A28E. The IP source binding table is taken as the basis for each interface to test received data packets. Figure 6-9 shows IP Source Guard principle.

- If the received IP packets meet the relationship of Port/IP/MAC/VLAN binding entries in IP source binding table, forward these packets.
- If the received IP packets are DHCP data packets, forward these packets.
- Otherwise, discard these packets.

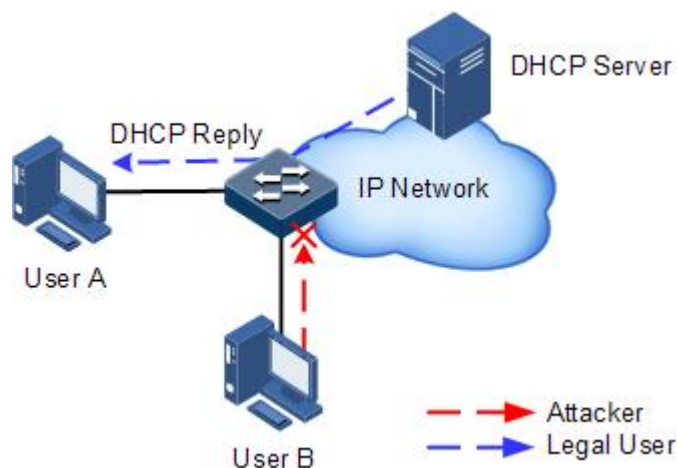


Figure 6-9 IP Source Guard principle

Before forwarding IP packets, the A10E/A28E compares the source IP address, source MAC address, interface ID, and VLAN ID of the IP packets with binding table information. If the information matches, it indicates that the user is legal and the packets are permitted to forward normally. Otherwise, the user is an attacker and the IP packets are discarded.

6.8.2 Preparing for configurations

Scenario

There are often some IP source spoofing attacks in network. For example, the attacker pretends legal users to send IP packets to the server, or the attacker forges the source IP address of another user to communicate. This makes the legitimate users cannot get network services normally.

With IP Source Guard binding, you can filter and control packets forwarded by the interface, prevent the illegal packets passing through the interface, thus to restrict the illegal use of network resources and improve the interface security.

Prerequisite

Enable DHCP Snooping before if there is a DHCP user.

6.8.3 Default configurations of IP Source Guard

The default configuration of IP Source Guard is as below.

Function	Default value
IP Source Guide static binding	Disable
IP Source Guide dynamic binding	Disable
Interface trust status	Untrusted

6.8.4 Configuring interface trust status of IP Source Guard

Configure interface trust status of IP Source Guard for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# ip verify source trust	Configure the interface to a trusted interface.

6.8.5 Configuring IP Source Guide binding

Configuring static IP Source Guide binding

Configure IP Source Guide static binding for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip verify source	Enable static IP Source Guide binding.
3	Alpha-A28E(config)# ip source binding <i>ip-address</i> [<i>mac-address</i>] [vlan <i>vlan-id</i>] port <i>port-id</i>	Configure static binding relationship.



Note

- The configured static binding relationship does not take effect when global static binding is disabled. Only when global static binding is enabled, the static binding relationship takes effect.
- For an identical IP address, the manually-configured static binding relationship will cover the dynamic binding relationship. However, it cannot cover the existing static binding relationship. When the static binding relationship is deleted, the system will recover the covered dynamic binding relationship automatically.

Configuring dynamic IP Source Guide binding

Configure IP Source Guide dynamic binding for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ip verify source { dhcp-snooping dhcp-relay }	Enable IP Source Guide dynamic binding.



Note

- The dynamic binding relationship learnt through DHCP Snooping does not take effect when global dynamic binding is disabled. Only when global dynamic binding is enabled, the dynamic binding relationship takes effect.
- If an IP address exists in the static binding table, the dynamic binding relationship does not take effect. In addition, it cannot cover the existing static binding relationship.

Configuring binding relationship translation

Configure binding relationship translation for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# ip verify source { dhcp-snooping dhcp-relay }	Enable IP Source Guide dynamic binding.
3	Alpha-A28E(config)# source binding { dhcp-snooping dhcp-relay } static	Translate the dynamic binding relationship to the dynamic binding relationship.
4	Alpha-A28E(config)# source binding auto-update	(Optional) enable auto-translation. After it is enabled, dynamic binding entries learned through DHCP Snooping are directly translated into static binding entries.

6.8.6 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show ip verify source	Show global binding status and interface trusted status.
2	Alpha-A28E# show ip source binding [port port-id]	Show configurations of IP Source Guard binding, interface trusted status, and binding relationship table.

6.8.7 Example for configuring IP Source Guard

Networking requirements

As shown in Figure 6-10, to prevent IP address embezzlement, you need to configure IP Source Guard on the switch.

- The switch permits all IP packets on Port 1 to pass.
- Port 2 permits IP packets with specified the IP address 10.10.10.1 and subnet mask 255.255.255.0 and the IP packets meeting DHCP Snooping learnt dynamic binding relationship to pass.
- Other interfaces only permit the packets meeting DHCP Snooping learnt dynamic binding relationship to pass.

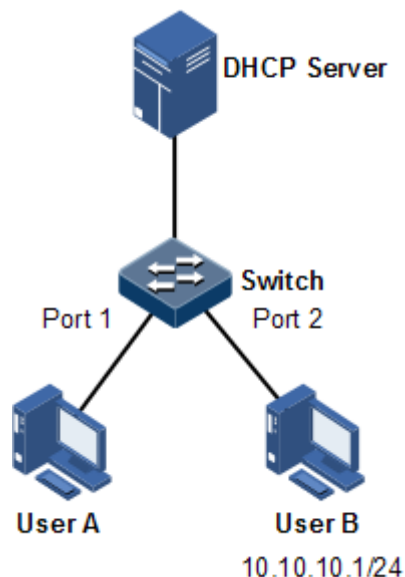


Figure 6-10 Configuring IP Source Guard

Configuration steps

Step 1 Set Port 1 to a trusted interface.

```
Alpha-A28E#config
Alpha-A28E(config)#interface port 1
Alpha-A28E(config-port)#ip verify source trust
Alpha-A28E(config-port)#exit
```

Step 2 Configure the static binding relationship.

```
Alpha-A28E(config)#ip verify source
Alpha-A28E(config)#ip source binding 10.10.10.1 port 2
```

Step 3 Enable global dynamic IP Source Guard binding.

```
Alpha-A28E(config)#ip verify source dhcp-snooping
```

Checking results

Show static binding table configurations by the command of **show ip source binding**.

```
Alpha-A28E#show ip source binding
History Max Entry Num: 1
```

```
Current Entry Num: 1
Ip Address      Mac Address    VLAN  Port  Type      Inhw
-----
10.10.10.1     --            --    2    static    yes
```

Show interface trusted status and IP Source Guard static/dynamic binding configurations by the command of **show ip verify source**.

```
Alpha-A28E#show ip verify source
```

```
Static Bind: Enable
Dhcp-Snooping Bind: Enable
Dhcp-Relay Bind: Disable
Port      Trust
-----
1         yes
2         no
3         no
...
```

6.9 PPPoE+

6.9.1 Introduction

PPPoE Intermediate Agent (PPPoE+) is used in processing of authentication packet. PPPoE+ adds device information into the authentication packet to bind account and access device so that the account is not shared and stolen, and the carrier's and users' interests are protected. This will give the server enough information to identify users, avoiding account sharing and theft and ensuring the network security.

With PPPoE dial-up mode, you can access the network through various interfaces of the device only when one authentication is successfully. However, the server cannot accurately differentiate users just by the authentication information, which contains the user name and password. With PPPoE+, besides the user name and the password, other information, such as the interface ID, is included in the authentication packet for authentication. If the interface ID identified by the authentication server cannot match with the configured one, authentication fails. This helps prevent illegal users from stealing accounts of other legal users for accessing the network.

The PPPoE protocol adopts C/S mode, as shown in Figure 6-11. The switch acts as a relay agent. Users access the network through PPPoE authentication. If the PPPoE server needs to locate users, more information should be contained in the authentication packet.

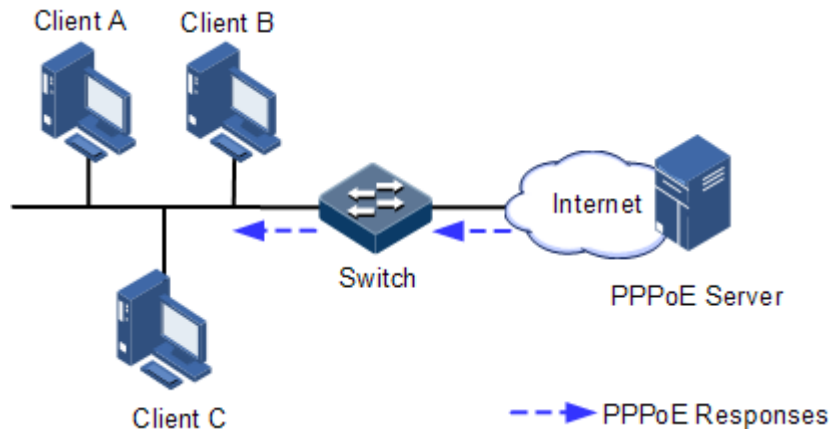


Figure 6-11 Accessing the network through PPPoE authentication

To access the network through PPPoE authentication, you need to pass through the following 2 stages: discovery stage (authentication stage) and session stage. PPPoE+ is used to process packets at the discovery stage. The following steps show the whole discovery stage.

- To access the network through PPPoE authentication, the client sends a broadcast packet PPPoE Active Discovery Initiation (PADI). This packet is used to query the authentication server.
- After receiving the PADI packet, the authentication server replies a unicast packet PPPoE Active Discovery Offer (PADO).
- If multiple authentication servers reply PADO packets, the client selects one from them and then sends a unicast PPPoE Active Discovery Request (PADR) to the authentication server.
- After receiving the PADR packet, if the authentication server believes that the user is legal, it sends a unicast packet PPPoE Active Discovery Session-confirmation (PADS) to the client.

PPPoE is mainly used to add user identification information in to PADI and PADR. Therefore, the server can identify whether the user identification information is identical to the user account for assigning resources.

6.9.2 Preparing for configurations

Scenario

To prevent illegal client access during PPPoE authentication, you need to configure PPPoE+ to add additional user identification information in PPPoE packet for network security.

Because the added user identification information is related to the specified switch and interface, the authentication server can bind the user with the switch and interface to effectively prevent account sharing and theft. In addition, this helps locate users to ensure network security.

Prerequisite

N/A

6.9.3 Default configurations of PPPoE+

The default configuration of I PPPoE+ is as below.

Function	Default value
Global PPPoE	Disable
Interface PPPoE	Disable
Padding mode of Circuit ID	Switch
Circuit ID information	Interface ID/VLAN ID/attached string
Attached string of Circuit ID	hostname
Padded MAC address of Remote ID	MAC address of the switch
Padding mode of Remote ID	Binary
Interface trusted status	Untrusted
Tag overriding	Disable



Note

By default, PPPoE packet is forwarded without being attached any information.

6.9.4 Configuring basic functions of PPPoE+



Caution

PPPoE+ is used to process PADI and PADR packets. It is designed for the PPPoE client. In general, PPPoE+ is only enabled on interfaces that are connected to the PPPoE client. Trusted interfaces are interfaces through which the switch is connected to the PPPoE server. PPPoE+ and trusted interface are exclusive. An interface is either enabled with PPPoE+ or is a trusted interface.

Enabling PPPoE+

After interface PPPoE+ is enabled, PPPoE authentication packets sent to the interface will be attached with user information and then are forwarded to the trusted interface.

Enable PPPoE+ for the A10E/A28E as below.

Step	Configuration	Description
1	<code>Alpha-A28E#config</code>	Enter global configuration mode.
2	<code>Alpha-A28E(config)#interface port port-id</code>	Enter physical layer interface configuration mode.
3	<code>Alpha-A28E(config- port)#pppoeagent enable</code>	Enable interface PPPoE+.

Configuring PPPoE trusted interface

PPPoE trusted interface can be used to prevent PPPoE server from being cheated and avoid security problems because PPPoE packets are forwarded to other non-service interfaces. In general, the interface connected to the PPPoE server is set to the trusted interface. PPPoE packets from the PPPoE client to the PPPoE server are forwarded by the trusted interface only. In addition, only PPPoE received from the trusted interface can be forwarded to the PPPoE client.

Configure PPPoE trusted interface for the A10E/A28E as below.

Step	Configuration	Description
1	<code>Alpha-A28E#config</code>	Enter global configuration mode.
2	<code>Alpha-A28E(config)#interface port port-id</code>	Enter physical layer interface configuration mode.
3	<code>Alpha-A28E(config-port)#pppoeagent trust</code>	Configure PPPoE trusted interfaces.



Note

Because PPPoE+ is designed for the PPPoE client instead of the PPPoE server, downlink interfaces of the device cannot receive the PADO and PADS packets. It means that interfaces, where PPPoE+ is enabled, should not receive PADO and PADS packet. If there interfaces receive these packets, it indicates that there are error packets and the packets should be discarded. However, these interfaces can forward PADO and PADS packets of trusted packet. In addition, PADI and PADR packets are forwarded to the trusted interface only.

6.9.5 Configuring PPPoE+ packet information

PPPoE is used to process a specified Tag in the PPPoE packet. This Tag contains Circuit ID and Remote ID.

- Circuit ID: is padded with the VLAN ID, interface ID, and host name of request packets at the RX client.
- Remote ID: is padded with the MAC address of the client or the switch.

Configuring Circuit ID

The Circuit ID has 2 padding modes: Switch mode and ONU mode. By default, Switch mode is adopted. In ONU mode, the Circuit ID has a fixed format. The following commands are used to configure the padding contents of the Circuit ID in Switch mode.

In switch mode, the Circuit ID supports 2 padding modes:

- Default mode: when customized Circuit ID is not configured, the padding content is the VLAN ID, interface ID, or the attached string. If the attached string is not defined, it is set to hostname by default.
- Customized mode: when customized Circuit ID is configured, the padding content is the Circuit IS string.

Configure Circuit ID for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# pppoeagent circuit-id mode { onu switch }	Configure the padding mode of the Circuit ID.
3	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
4	Alpha-A28E(config-port)# pppoeagent circuit-id string	(Optional) set the Circuit ID to the customized string.

In default mode, the Circuit ID contains an attached string. By default, the attached string is set to the hostname of the switch. You can set it to a customized string.

Configure the attached string of the Circuit ID for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# pppoeagent circuit-id attach-string string	(Optional) configure the attached string of the Circuit ID. If the Circuit ID is in default mode, attached string configured by this command will be added to the Circuit ID.

Configuring Remote ID

The Remote ID is padded with a MAC address of the switch or a client. In addition, you can specify the form (binary/ASCII) of the MAC address.

Configure Remote ID for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# pppoeagent remote-id { client-mac switch-mac }	(Optional) configure PPPoE+ Remote ID to be padded with the MAC address.
4	Alpha-A28E(config-port)# pppoeagent remote-id format { ascii binary }	(Optional) configure the padding modes of the PPPoE+ Remote ID.

Configuring Tag overriding

Tags of some fields may be forged by the client because of some reasons. The client overrides the original Tags. After Tag overriding is enabled, if the PPPoE packets contain Tags, these Tags are overridden. If not, add Tags to these PPPoE packets.

Configure Tag overriding for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# pppoeagent vendor-specific-tag overwrite enable	Enable Tag overriding.

6.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show pppoeagent [port-list <i>port-list</i>]	Show PPPoE+ configurations.
2	Alpha-A28E# show pppoeagent statistic [port-list <i>port-list</i>]	Show PPPoE+ statistics.

6.9.7 Maintenance

You can maintain operating status and configurations on the PPPoE+ feature through the below command.

Command	Description
Alpha-A28E(config)# clear pppoeagent statistic [port-list <i>port-list</i>]	Clear PPPoE+ statistics.

6.9.8 Example for configuring PPPoE+

Networking requirements

As shown in Figure 6-12, to prevent illegal access during PPPoE authentication and to control and monitor users, you need to configure PPPoE+ on the switch.

- Port 1 and Port 2 are connected to Client 1 and Client 2 respectively. Port 3 is connected to the PPPoE server.
- Enable global PPPoE+ and enable PPPoE+ on Port 1 and Port 2. Set Port 3 to the trusted interface.

- Set the attached string of the Circuit ID to alpha-a28e. Set the padding content of the Circuit ID on Port 1 to user01. Set the padding content of the Remote ID on Port 2 to the MAC address of the client. The padding contents are in ASCII mode.
- Enable Tag overriding on Port 1 and Port 2.

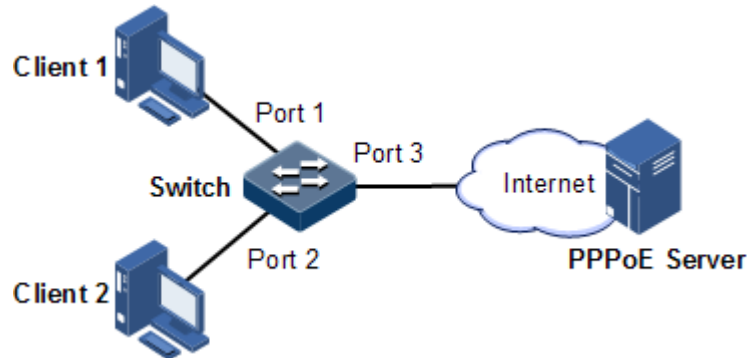


Figure 6-12 Configuring PPPoE+

Configuration steps

Step 1 Set Port 3 to the trusted interface.

```
Alpha-A28E#config
Alpha-A28E(config)#interface port 3
Alpha-A28E(config-port)#pppoenagent trust
Alpha-A28E(config-port)#exit
```

Step 2 Configure packet information of Port 1 and Port 2.

```
Alpha-A28E(config)#pppoenagent circuit-id attach-string alpha-a28e
Alpha-A28E(config)#interface port 1
Alpha-A28E(config-port)#pppoenagent circuit-id user01
Alpha-A28E(config-port)#exit
Alpha-A28E(config-port)#interface port 2
Alpha-A28E(config-port)#pppoenagent remote-id client-mac
Alpha-A28E(config-port)#pppoenagent remote-id format ascii
Alpha-A28E(config-port)#exit
```

Step 3 Enable Tag overriding on Port 1 and Port 2.

```
Alpha-A28E(config)#interface port 1
Alpha-A28E(config-port)#pppoenagent vendor-specific-tag overwrite enable
Alpha-A28E(config-port)#exit
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#pppoenagent vendor-specific-tag overwrite enable
Alpha-A28E(config-port)#exit
```


Step 4 Enable PPPoE+ on Port 1 and Port 2.

```
Alpha-A28E(config)#interface port 1
Alpha-A28E(config-port)#pppoeagent enable
Alpha-A28E(config-port)#exit
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#pppoeagent enable
```

Checking results

Show PPPoE+ configurations by the command of **show pppoeagent [port-list port-list]**.

```
Alpha-A28E#show pppoeagent port-list 1-3
Attach-string: alpha-a28e
Circuit ID padding mode: switch
Port   Enable Trust-port Overwrite Remote-ID   Format-rules Circuit-ID
-----
1      enable  no      enable  switch-mac  binary      user01
2      enable  no      enable  client-mac  ascii       %default%
3      disable yes     disable switch-mac  binary       %default%
**In switch mode, Circuit-ID's default string is: Port\Vlan\Attach-string.
**In onu mode, Circuit-ID's default string is: 0 0/0/0:0.0
0/0/0/0/0/0/MAC 0/0/Port:eth/4096.CVLAN LN.
**Attach-string's default string is the hostname.
```

6.10 Loopback detection

6.10.1 Introduction

The interface loopback detection function solves the network effect, improves network error-detection, error tolerance and stability.

Procedure of loopback detection:

- Each interface of device sends loopback-detection message by interval (the interval is configurable, by default: 4s).
- The A10E/A28E checks source MAC field for interface received loopback detection packets, if the source MAC is identical to device MAC, then some interfaces of the device form a loop; otherwise, discard the message.
- If the packets Tx interface ID is identical to Rx interface ID, shutdown the interface;
- If the packets Tx interface ID is not identical to Rx interface ID, shutdown the interface with bigger ID, and leave the smaller interface ID in Up status.

Common loop types are self-loop, internal loop and external loop.

As shown in Figure 6-13, Switch B and Switch connect user network.

- Self-loop: user loop in the same Ethernet interface on the same device, user network B has loop itself, which forms self-loop;
- Internal loop: the loop formed in different Ethernet interfaces on the same device, Switch C interface 1 and interface 3 forms internal loop with the user network A;
- External loop: the loop formed in the Ethernet interface of different devices, Switch A, Switch B and Switch C form external loop with user network C.

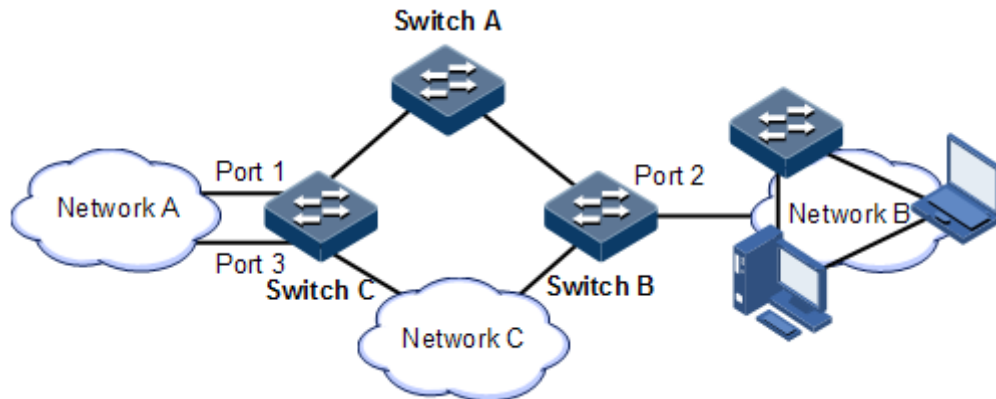


Figure 6-13 Loopback detection networking

In Figure 6-13, assume that both Switch B and Switch C connect user network interfaces enable loop detection function. The loop detection processing mechanism for the three loop types are as follows:

- Self-loop: the No. of the interface to receive packets and that to send packet on Switch B are the same, shut down Port 2 and remove self-loop.
- Internal loop: Switch C will receive the loop detection packets issued by it and the Rx/Tx packets interface numbers are different, then shut down Port 3 with bigger interface ID, remove internal loop.
- External loop: Switch B and Switch C will receive the loop detection packets from each other; generally, loop detection does not deal with external loop, Switch B and Switch C only send Trap alarm without blocking. But you can configure to block one of the interfaces manually, such as block device interface with bigger MAC address so as to remove external loop.

6.10.2 Preparing for configurations

Scenario

In the network, the hosts or Layer 2 devices under access devices may form loop by network cable intentionally or involuntary. Enable loopback detection function at downlink interface of access device to avoid the network jam formed by unlimited copies of data flow caused by downlink interface loop. Block the loop interface once there is a loop.

Prerequisite

Configure interface physical parameters to make it Up before configuring loopback detection.

6.10.3 Default configurations of loopback detection

The default configuration of loopback detection is as below.

Function	Default value
Interface loopback detection function status	Disable
Automatic recovery time for interface block	No automatic recovery
Loop process mode of loopback detection	trap-only
Loopback detection period	4s
Loopback detection mode	VLAN mode
The automatic open blocked interface time for loopback detection	infinite
Loopback detection VLAN	VLAN 1


6.10.4 Configuring loopback detection



Note

- Loopback detection function and STP are exclusive, only one can be enabled at one time.
- The straight connection device cannot enable loopback detection in both ends simultaneously; otherwise the interfaces at both ends will be blocked.

Configure loopback detection function as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# loopback-detection { enable disable } port-list port-list	Enable loopback detection on the interface.
3	Alpha-A28E(config)# loopback-detectiondestination-address mac-address	(Optional) configure the destination MAC address of loopback detection packets.  Note Loopback detection in the entire topology must be configured the same; otherwise, loopback detection may fail.
4	Alpha-A28E(config)# loopback-detection vlan vlan-id	(Optional) configure loopback detection VLAN.
5	Alpha-A28E(config)# loopback-detection hello-time period	Configure the period for sending loopback detection packets.
6	Alpha-A28E(config)# loopback-detection error-device { discarding trap-only } port-list port-list	(Optional) configure process mode when the interface receives loopback detection message from other devices.

Step	Configuration	Description
7	Alpha-A28E(config)# loopback-detection down-time { <i>time-value</i> trap-only infinite }	(Optional) configure the automatic open blocked interface time for loopback detection.
8	Alpha-A28E(config)# interface port <i>port-id</i> Alpha-A28E(config-port)# no loopback-detection discarding	Enable the interface blocked by loopback detection.

6.10.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show loopback-detection port-list <i>port-list</i>	Show interface loopback detection configuration.
2	Alpha-A28E# show loopback-detection statistics port-list <i>port-list</i>	Show statistics of loopback detection.

6.10.6 Maintenance

Maintain the A10E/A28E by below commands.

Command	Description
Alpha-A28E(config-port)# clear loopback-detection statistic	Clear loopback detection statistics.

6.10.7 Example for configuring loopback detection

Networking requirements

As shown in Figure 6-14, Port 1 of Switch A is connected to core network; Port 2 and Port 3 of Switch A are connected to user network. There is loop in user network. Enable loopback detection function on Switch A to detect loop in user network and then can block the related port.

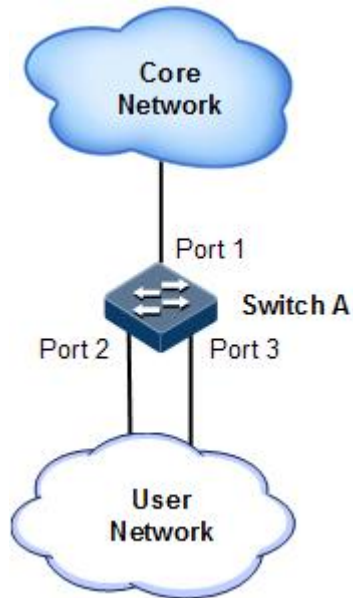


Figure 6-14 Loopback detection application

Configuration steps

Step 1 Create VLAN 3 and add Port 2 and Port 3 into VLAN 3.

```
Alpha-A28E#config
Alpha-A28E(config)#create vlan 3 active
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#switchport access vlan 3
Alpha-A28E(config-port)#exit
Alpha-A28E(config)#interface port 3
Alpha-A28E(config-port)#switchport access vlan 3
Alpha-A28E(config-port)#exit
```

Step 2 Enable loopback detection for the specified interface.

```
Alpha-A28E(config)#loopback-detection enable port-list 2-3
Alpha-A28E(config)#loopback-detection vlan 3
Alpha-A28E(config)#loopback-detection hello-time 3
```

Checking configurations

Use the **show loopback-detection** command to show interface loopback detection status.

```
Alpha-A28E#show loopback-detection port-list 2-3
Destination address: FFFF.FFFF.FFFF
VLAN: 3
```

```

Period of loopback-detection:3s
Restore time:infinite
Port State Status exloop-act Last Last-Occur Open-Time vlan
          Loop-with (ago) (ago)
-----
2      Ena   no   trap-only  --      --      --      --
3      Ena   no   trap-only  --      --      --      --
    
```

6.11 Line detection

6.11.1 Introduction

Line detection is a module to detect physical lines and provides you with status query function, so it can help you analyze fault source and maintain the network.

6.11.2 Preparing for configurations

Scenario

With this function, you can query status of physical lines between devices, analyze faults, and thus maintain the network.

Prerequisite

N/A

6.11.3 Configuring line detection

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# test cable-diagnostics port-list { all port-list }	Detect physical link status.

6.11.4 Checking configurations

Use the following command to check configuration result.

No.	Item	Description
1	Alpha-A28E# show cable-diagnostics port-list { all port-list }	Show information about line detection.

6.11.5 Example for configuring line detection

Networking requirements

As shown in Figure 6-15, to help you analyze fault source, detect lines with the switch.

No line detection is done before.

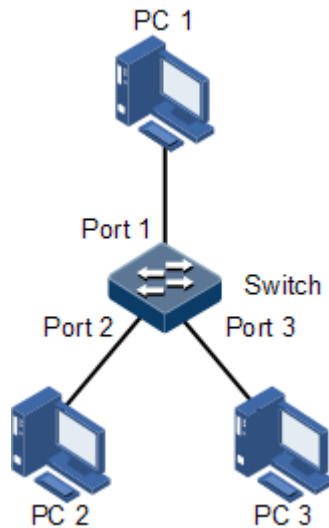


Figure 6-15 Line detection application networking

Configuration steps

Perform line detection on Ports 1–3 on the A10E/A28E.

```
Alpha-A28E#test cable-diagnostics port-list 1-3
```

Checking results

Use **show cable-diagnostics port-list [all | port-list]** command to check whether Port 1 and Port 2 on the A10E/A28E are correctly configured.

```
Alpha-A28E#show cable-diagnostics port-list 1-2
Port Attribute      Time           RX Stat  RX Len(m)  TX Stat  TX Len(m)  ----
-----
1   Issued   01/09/2011 08:13:03  Normal   0          Normal   0
2   Issued   01/09/2011 08:13:03  Normal   0          Normal   0
```

Remove the line that connects PC 1 and the A10E/A28E from the PC 1, and perform line detection again. Use the **show cable-diagnostics port-list [all | port-list]** command to check whether line detection is correctly configured.

Alpha-A28E#show cable-diagnostics port-list 1-2

Port	Attribute	Time	RX Stat	RX Len(m)	TX Stat	TX Len(m)
1	Issued	01/09/2011 08:18:09	Open	3	Open	3
2	Issued	01/09/2011 08:18:09	Normal	0	Normal	0

7 Reliability

This chapter introduces basic principle and configuration of reliability and provides related configuration applications.

- Link aggregation
- Interface backup
- Failover
- STP
- MSTP
- ERPS
- RRPS

7.1 Link aggregation

7.1.1 Introduction

With link aggregation, multiple physical Ethernet interfaces are combined to form a logical aggregation group. Multiple physical links in one aggregation group are taken as a logical link. The link aggregation helps share traffics among members in an aggregation group. In addition to effectively improve the reliability on links between devices, the link aggregation can help gain higher bandwidth without upgrading hardware.

In general, the link aggregation consists of manual link aggregation, static Link Aggregation Control Protocol (LACP) link aggregation, and dynamic LACP link aggregation.

- Manual link aggregation

Manual link aggregation refers to a process that multiple physical interfaces are aggregated to a logical interface. Links under a logical interface share loads.

- Static LACP link aggregation

Link Aggregation Control Protocol (LACP) is a protocol based on IEEE802.3ad. LACP communicates with the peer through the Link Aggregation Control Protocol Data Unit (LACPDU). In addition, you should manually configure the link aggregation group. After LACP is enabled on an interface, the interface sends a LACPDU to inform the peer of its

system LACP protocol priority, system MAC address, interface LACP priority, interface ID, and operation Key.

After receiving the LACPDU, the peer compares its information with the one received by other interfaces to select a selected interface. Therefore, the interface and the peer are in the same Selected state. The operation key is a configuration combination automatically generated based on configurations of the interface, such as the speed, duplex mode, and Up/Down status. In a link aggregation group, interfaces in the Selected state share the identical operation key.

- Dynamic LACP link aggregation

In dynamic LACP link aggregation, the system automatically creates and deletes the link aggregation group and member interfaces through LACP. Interfaces cannot be automatically aggregated into a group unless their basic configurations, speeds, duplex modes, connected devices, and the peer interfaces are identical.

In manual aggregation mode, all member interfaces are in forwarding state, sharing loads. In static/dynamic LACP mode, there are backup links.

Link aggregation is the most widely-used and simplest Ethernet reliability technology.



Note

The A10E/A28E supports manual and static link aggregation only.

7.1.2 Preparing for configurations

Scenario

When needing to provide higher bandwidth and reliability for a link between two devices, you can configure the link aggregation.

With link aggregation, multiple physical Ethernet ports are added to a Trunk group and are aggregated to a logical link. The link aggregation helps sharing uplink and downlink traffics among members in one aggregation group. Therefore, the link aggregation helps get higher bandwidth and helps members in one aggregation group back up data for each other, which improving the reliability of Ethernet connection.

Prerequisite

Before configuring link aggregation, you need to configure physical parameters on a port and make the physical layer **Up**.

7.1.3 Default configurations of link aggregation

The default configuration of link aggregation is as below.

Function	Default value
Link aggregation	Enable
Load balancing mode	sxordmac
Link aggregation group	Existing, in manual mode
LACP system priority	32768

Function	Default value
LACP interface priority	LACP priority without specifying interface
Interface dynamic LACP link aggregation	Disable

7.1.4 Configuring manual link aggregation

Configure manual link aggregation for the A10E/A28E as below.

Step	Configuration	Description
1	<code>Alpha-A28E#config</code>	Enter global configuration mode.
2	<code>Alpha-A28E(config)#trunk group <i>group-id</i> port <i>port-list</i></code>	Configure link aggregation group.
3	<code>Alpha-A28E(config)#trunk enable</code>	Enable link aggregation group.
4	<code>Alpha-A28E(config)#trunk loading-sharing mode { dip dmac sip smac sxordip sxordmac }</code>	(Optional) configure load sharing mode for link aggregation.



Note

In the same link aggregation group, member interfaces that share loads must be identically configured. These configurations include QoS, QinQ, VLAN, interface properties, and MAC address learning.

- QoS: traffic policing, rate limit, SP queue, WRR queue scheduling, interface priority and interface trust mode.
- QinQ: QinQ enabling/disabling status on the interface, added outer VLAN tag, policies for adding outer VLAN Tags for different inner VLAN IDs.
- VLAN: the allowed VLAN, default VLAN and the link type (Trunk or Access) on the interface, subnet VLAN configurations, protocol VLAN configurations, and whether VALN packets carry Tag.
- Port properties: whether the interface is added to the isolation group, interface rate, duplex mode, and link Up/Down status.
- MAC address learning: whether enabling the MAC address learning, and whether the MAC address limit is configured on the interface.

7.1.5 Configuring static LACP link aggregation

Configure static LACP link aggregation for the A10E/A28E as below.

Step	Configuration	Description
1	<code>Alpha-A28E#config</code>	Enter global configuration mode.

Step	Configuration	Description
2	Alpha- A28E(config)# lACP system-priority <i>system-priority</i>	(Optional) configure system LACP priority. The higher priority end is active end. LACP chooses active and backup interfaces according to the active end configuration. The smaller the number is, the higher the priority is. The smaller system MAC address device will be chosen as active end if devices system LACP priorities are identical.
3	Alpha- A28E(config)# lACP timeout { fast slow }	Configure LACP timeout mode.
4	Alpha- A28E(config)# trunk group group-id port port-list [lACP- static]	Create a static LACP link aggregation group.
5	Alpha- A28E(config)# interfac e port port-id	(Optional) enter physical layer interface configuration mode.
6	Alpha-A28E(config- port)# lACP port- priority port- <i>priority</i>	(Optional) configure LACP priority on the interface. It affects electing the default interface of LACP. The smaller the value is, the higher the priority is.
7	Alpha-A28E(config- port)# lACP mode { active passive }	(Optional) configure LACP mode for member interfaces. If both two ends of a link are in passive mode, LACP connection cannot be established.
8	Alpha-A28E(config- port)# exit	Return to global configuration mode.
9	Alpha- A28E(config)# trunk enable	Enable link aggregation group.
10	Alpha- A28E(config)# trunk loading-sharing mode { dip dmac sip smac sxordip sxordmac }	(Optional) configure load sharing mode for the aggregation link.
11	Alpha- A28E(config)# trunk group group-id min- active links <i>threshold</i>	(Optional) configure the minimum number of active links in LACP link aggregation group.

 **Note**

- Interface in static LACP link aggregation group can be in active or standby status. Both active interface and standby interface can receive/transmit LACP packets, but standby interface cannot forward client packets.

- System chooses default interface in the order of neighbor discovery, interface maximum speed, interface highest LACP priority, and interface minimum ID. The interface is in active status by default, the interface with identical speed, identical peer and identical device operation key is also in active status; other interfaces are in standby status.

7.1.6 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show lacp internal	Show local LACP interface status, tag, interface priority, administration key, operation key, and interface status machine status.
2	Alpha-A28E# show lacp neighbor	Show the peer LACP information, including tag, interface priority, device ID, Age, operation key value, interface ID, and interface status machine status.
3	Alpha-A28E# show lacp statistics	Show interface LACP statistics, including total number of received/sent LACP packets, the number of received/sent Marker packets, the number of received/sent Marker Response packets, the number of errored Marker Response packets,
4	Alpha-A28E# show lacp sys-id	Show global LACP enabling status of the local system, device ID, including system LACP priority and system MAC address.
5	Alpha-A28E# show trunk	Show configurations of all link aggregation groups.

7.1.7 Example for configuring manual link aggregation

Networking requirements

As shown in Figure 7-1, to improve link reliability between Switch A and Switch B, you should configure manual link aggregation for the two devices. Add Port 1 and Port 2 into link aggregation group to build up a unique logical interface. The link aggregation group performs load sharing according to the source MAC address.

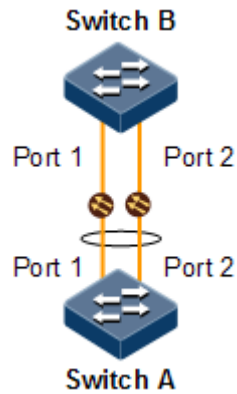


Figure 7-1 Configuring manual link aggregation

Configuration steps

Step 1 Create a manual link aggregation group.

Configure Switch A.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#trunk group 1 port 1-2
```

Configure Switch B.

```
Alpha-A28E#hostname SwitchB
SwitchB#config
SwitchB(config)#trunk group 1 port 1-2
```

Step 2 Configure the load sharing mode for aggregated links.

Configure Switch A.

```
SwitchA(config)#trunk loading-sharing mode smac
```

Configure Switch B.

```
SwitchB(config)#trunk loading-sharing mode g smac
```

Step 3 Enable link aggregation.

Configure Switch A.

```
SwitchA(config)#trunk enable
```

Configure Switch B.

```
SwitchB(config)#trunk enable
```

Checking results

Show global configurations on manual link aggregation by the command of **show trunk**.

```
SwitchA#show trunk
Trunk: Enable
Loading sharing mode: SMAC
Trunk Group Mode  Member Ports          Efficient Ports
-----
1                 manual 1,2                1,2
```

7.1.8 Example for configuring static LACP link aggregation

Networking requirements

As shown in Figure 7-2, to improve link reliability between Switch A and Switch B, you can configure a static LACP link aggregation between these 2 devices. Add Port 1 and Port 2 into one link aggregation group, where Port 1 is used as the current link and Port 2 is the protection link.

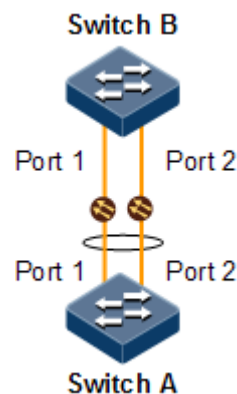


Figure 7-2 Configuring static LACP link aggregation

Configuration steps

- Step 1 Configure the static LACP link aggregation group on Switch A and set Switch A to the active end.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#trunk group 1 port 1-2 lacp-static
SwitchA(config)#lacp system-priority 1000
SwitchA(config)#trunk group 1 min-active links 1
SwitchA(config)#interface port 1
SwitchA(config-port)#lacp port-priority 1000
SwitchA(config-port)#exit
SwitchA(config)#trunk enable
```

- Step 2 Configure the static LACP link aggregation group on Switch B.

```
Alpha-A28E#hostname SwitchB
SwitchB#config
SwitchB(config)#trunk group 1 port 1-2 lacp-static
SwitchB(config)#lacp system-priority 1000
SwitchB(config)#trunk enable
```

Checking results

Show global configurations on static LACP link aggregation on Switch A by the command of **show trunk**.

```
SwitchA#show trunk
Trunk: Enable
Loading sharing mode: SMAC
Trunk Group Mode  Member Ports          Efficient Ports
-----
1          static 1,2                --
```

Show local system LACP interface state, flag, interface priority, administration key, operation key, and interface state machine state on Switch A by the command of **show lacp internal**.

```
SwitchA#show lacp internal
Flags:
  S - Device is requesting Slow LACPDUS
  F - Device is requesting Fast LACPDUS
  A - Device is in Active mode
  P - Device is in Passive mode
Port State      Flags Port-Pri  Admin-key Oper-key Port-State
-----
1  down        FA   1000      0x1      0x1      0xF
```



```
2    down    FA    32768    0x1    0x1    0xF
```

Show peer system LACP interface state, flag, interface priority, administration key, operation key, and interface state machine state on Switch A by the command of **show lacp neighbor**.

7.2 Interface backup

7.2.1 Introduction

In dual uplink networking, Spanning Tree Protocol (STP) is used to block the redundancy link and implements backup. Though STP can meet users' backup requirements, but fails to meet switching requirements. Though Rapid Spanning Tree Protocol (RSTP) is used, the convergence is second level only. This is not a satisfying performance parameter for high-end Ethernet switch which is applied to the Carrier-grade network core.

Interface backup, targeted for dual uplink networking, implements redundancy backup and quick switching through working and protection links. It ensures performance and simplifies configurations.

Interface backup is another solution of STP. When STP is disabled, you can realize basic link redundancy by manually configuring interfaces. If the switch is enabled with STP, you should disable interface backup because STP has provided similar functions.

Principles

Interface backup is realized by configuring the interface backup group. Each interface backup group contains a primary interface and a backup interface. The link, where the primary interface is, is called a primary link while the link, where the backup interface is, is called the backup interface. Member interfaces in the interface backup group supports physical interfaces and link aggregation groups. However, they do not support Layer 3 interfaces.

In the interface backup group, when an interface is in Up status, the other interface is in Standby status. At any time, only one interface is in Up status. When the Up interface fails, the Standby interface is switched to the Up status.

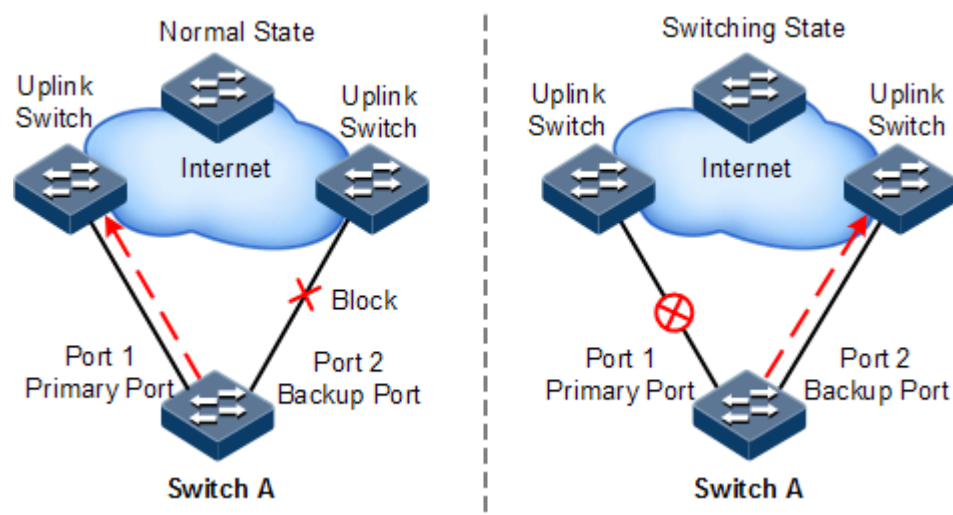


Figure 7-3 Principles of interface backup

As shown in Figure 7-3, Port 1 and Port 2 on Switch A are connected to their uplink devices respectively. The interface forwarding states are shown as below:

- Under normal conditions, Port 1 is the primary interface while Port 2 is the backup interface. Port 1 and the uplink device forward packet while Port 2 and the uplink device do not forward packets.
- When the link between Port 1 and its uplink device fails, the backup Port 2 and its uplink device forward packets.
- When Port 1 restores normally and keeps Up for a period (restore-delay), Port 1 restores to forward packets and Port 2 restores standby status.

When a switching between the primary interface and the backup interface occurs, the switch sends a Trap to the NView NNM system.

Application of interface backup in different VLANs

By applying interface backup to different VLANs, you can enable two interfaces to share service load in different VLANs, as shown in Figure 7-4.

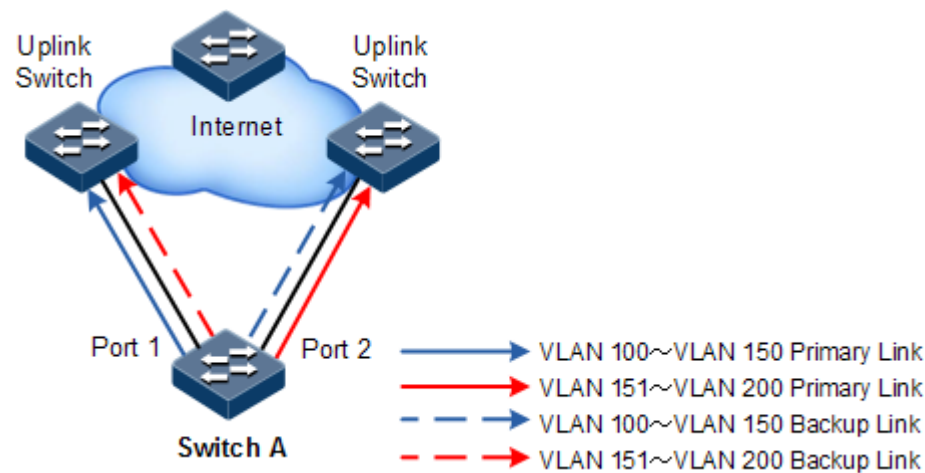


Figure 7-4 Application of interface backup in different VLANs

In different VLANs, the forwarding status is shown as below:

- Under normal conditions, configure Switch A in VLANs 100–150.
- In VLANs 100–150, Port 1 is the primary interface and Port 2 is the backup interface.
- In VLANs 151–200, Port 2 is the primary interface and Port 1 is the backup interface.
- Port 1 forwards traffic of VLANs 100–150, and Port 2 forwards traffic of VLANs 151–200.
- When Port 1 fails, Port 2 forwards traffic of VLANs 100–200.
- When Port 1 restores normally and keeps Up for a period (restore-delay), Port 1 forwards traffic of VLANs 100–150, and Port 2 forwards VLANs 151–200.

Interface backup is used share service load in different VLANs without depending on configurations of uplink switches, thus facilitating users' operation.

7.2.2 Preparing for configurations

Scenario

When STP is disabled, by configuring interface backup, you can realize redundancy backup and fast switching of primary/backup link, and load sharing between different interfaces.

Compared with STP, interface backup not only ensures millisecond level fast switching, also simplifies configurations.

Prerequisite

- Create VLANs.
- Add interfaces to VLANs.
- Disable STP.

7.2.3 Default configurations of interface backup

The default configuration of interface backup is as below.

Function	Default value
Interface backup group	None
Restore-delay	15s
Restoration mode	Interface connection mode (port-up)

7.2.4 Configuring basic functions of interface backup

Configure basic functions of interface backup for the A10E/A28E as below.



Caution

Interface backup and STP, loopback detection, Ethernet ring, or ELPS, and ERPS may interfere with each other. Configuring both of them on an interface is not recommended.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# switchport backup port port-id [vlanlist vlan-list]	Configure the interface backup group.
4	Alpha-A28E(config-port)# exit	Return to global configuration mode.
5	Alpha-A28E(config)# switchport backup restore-delay period	(Optional) configure the restore-delay period.

Step	Configuration	Description
6	Alpha-A28E(config)# switchport backup restore-mode { disable neighbor-discover port-up }	(Optional) configure restoration mode.



Note

- In an interface backup group, an interface is either a primary interface or a backup interface.
- In a VLAN, an interface or a link aggregation group cannot be a member of two interface backup groups simultaneously.
- If you set a link aggregation group as a member of interface backup group, you need to set the member with the minimum interface ID in the link aggregation group as the member. When the member is in Up status, this indicates that the link aggregation group has a Up interface. When the member is in Down status, this indicates that all interfaces in the link aggregation group are Down.

7.2.5 (Optional) configuring force switching on interfaces



Caution

- After force switching is successfully configured, the primary/backup link will be switched; namely, the current link is switched to the backup link (without considering Up/Down status of the primary/backup interface). For example, when both the primary interface and backup interface are in Up status, the primary link transmits data. In this situation, if you perform forcible switchover, the working link changes from the primary link to the backup link.
- In the force switching command, the backup interface number is optional. If the primary interface is configured with multiple interface backup groups, you should input the backup interface ID.

Configure force switching on interfaces for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# switchport backup [port port-id] force-switch	Configure force switching on the interface.

7.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show switchport backup	Show related status information of interface backup, including restoration delay time, restoration mode, and interface backup groups.

7.2.7 Example for configuring interface backup

Networking requirements

When only link aggregation is configured, all VLAN data comes from only one interface, where packet discarding occurs and services are impacted. In this situation, you can configure two link aggregation groups to sharing VLAN data to two interfaces so that load balancing can work and the protection feature of link aggregation groups can be inherited.

As shown in Figure 7-5, the PC accesses the server through switches. To realize a reliable remote access from the PC to the server, configure an interface backup group on Switch A and specify the VLAN list so that the two interfaces concurrently forward services in different VLANs and share load. Configure Switch A as below:

- Switch A is in VLANs 100–150. Port 1 is the primary interface and Port 2 is the backup interface.
- Switch A is in VLANs 151–200. Port 2 is the primary interface and Port 1 is the backup interface.

When Port 1 or its link fails, the system switches to the backup Port 2 to resume the link.

Switch A should support interface backup while Switch B, Switch C, and Switch D do not need to support interface backup.

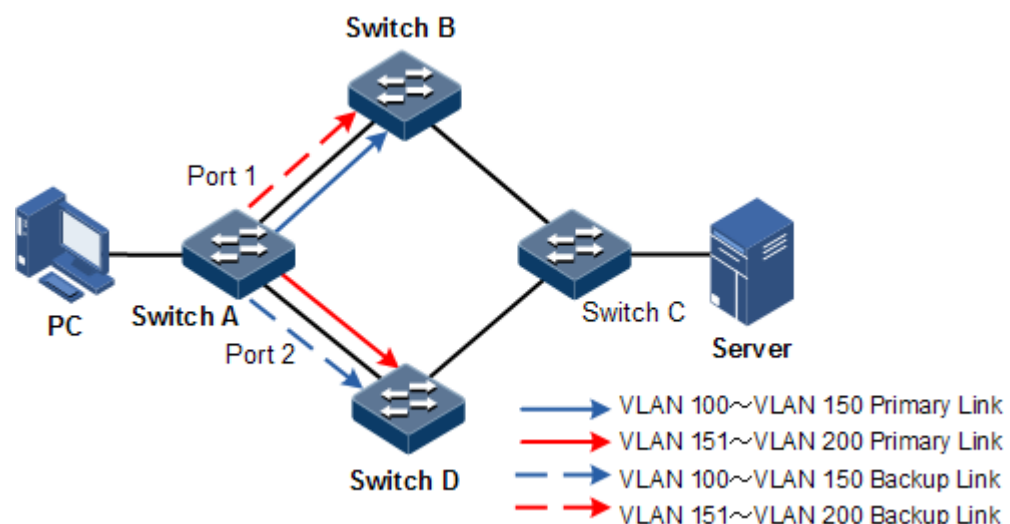


Figure 7-5 Configuring interface backup

Configuration steps

- Step 1 Create VLANs 100–200 and add Port 1 and Port 2 to VLANs 100–200.

```
Alpha-A28E#config
Alpha-A28E(config)#create vlan 100-200 active
Alpha-A28E(config)#interface port 1
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk allowed vlan 100-200 confirm
Alpha-A28E(config-port)#exit
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#switchport mode trunk
Alpha-A28E(config-port)#switchport trunk allowed vlan 100-200 confirm
Alpha-A28E(config-port)#exit
```

Step 2 Set Port 1 to the primary interface and set Port 2 to the backup interface in VLANs 100–150.

```
Alpha-A28E(config)#interface port 1
Alpha-A28E(config-port)#switchport backup port 2 vlanlist 100-150
Alpha-A28E(config-port)#exit
```

Step 3 Set Port 2 to the primary interface and set Port 1 to the backup interface in VLANs 151–200.

```
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#switchport backup port 1 vlanlist 151-200
```

Checking results

Use the **show switchport backup** command to view status of interface backup under normal or faulty conditions.

When both Port 1 and Port 2 are Up, Port 1 forwards traffic of VLANs 100–150, and Port 2 forwards traffic of VLANs 151–200.

```
Alpha-A28E#show switchport backup
Restore delay: 15s.
Restore mode: port-up.
Active Port(State)    Backup Port(State)    vlanlist
-----
1      (Up)              2      (Standby)    100-150
2      (Up)              1      (Standby)    151-200
```

Manually disconnect the link between Switch A and Switch B to emulate a fault. Then, Port 1 becomes Down, and Port 2 forwards traffic of VLANs 100–200.

```
Alpha-A28E#show switchport backup
Restore delay: 15s
```

```
Restore mode: port-up
Active Port(State)  Backup Port(State)  Vlanlist
-----
1 (Down)           2 (Up)               100-150
2 (Up)             1 (Down)             151-200
```

When Port 1 resumes and keeps Up for 15s (restore-delay), it forwards traffic of VLANs 100–150 while Port 2 forwards traffic of VLANs 151–200.

7.3 Failover

7.3.1 Introduction

Failover is used to provide port linkage scheme for specific application and it can extend range of link backup. By monitoring uplinks and synchronizing downlinks, add uplink and downlink interfaces to a failover group. Therefore, faults of uplink devices can be informed to the downlink devices to trigger switching. Failover can be used to prevent traffic loss due to uplink failure.

Once all uplink interfaces fail, down link interfaces are in Down status. When at least one uplink interface recovers, downlink interface recovers to Up status. Therefore, faults of uplink devices can be informed to the downlink devices immediately. Uplink interfaces are not influenced when downlink interfaces fail.

7.3.2 Preparing for configurations

Scenario

When uplink fails, traffic cannot switch to standby link if it cannot notify downlink devices in time then traffic will be broken.

Failover can be used to add downlink interfaces and uplink interfaces of the middle device to a failover group and monitor uplink interfaces. When all uplink interfaces fails, faults of uplink devices can be informed to the downlink devices to trigger switching.

Prerequisite

Before configuring failover, connect interfaces and configure physical parameters for it. The interface is Up at physical layer.

7.3.3 Default configurations of failover

The default configuration of failover is as below.

Function	Default value
Failover group	N/A

7.3.4 Configuring failover

Configure failover for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# link-state-tracking group <i>group-number</i> { upstream cfm-mepid <i>mep-id</i> }	Create the failover group and enable failover.
3	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
4	Alpha-A28E(config-port)# link-state-tracking group <i>group-number</i> { downstream upstream }	Configure the failover group of the interface and interface type. One interface can only belong to one failover group and can be either the uplink interface or downlink interface. When the failover group is configured with CFM network or G.8031 network in uplink, the interface can be set to downlink interface only.



Note

- One failover group can contain several uplink interfaces. Failover will not be performed when at least one uplink interface is Up. Only when all uplink interfaces are Down, failover occurs.
- In global configuration mode, use the **no link-state-tracking group** *group-number* command to disable failover. The failover group will be deleted if there is no interface in it.
- Use the **no link-state-tracking group** command to delete an interface from the failover group in physical layer interface configuration mode. If there is no other interface and failover is disabled, the failover group will be deleted when the interface is deleted.

7.3.5 Checking configurations

Use the following commands to check configuration results.

Step	Configuration	Description
1	Alpha-A28E# show link-state-tracking group <i>group-number</i>	Show configurations and status of the failover group.
2	Alpha-A28E# show link-admin-status port <i>port-list</i>	Show interface Up/Down status configured on each functional module on the interface.

7.3.6 Example for configuring failover

Networking requirements

As shown in Figure 7-6, to improve network reliability, Link 1 and Link 2 of Switch B are connected to Switch A and Switch C respectively. Link 1 is the primary link and Link 2 is the standby link. Link 2 will not be used to forward data until Link 1 is fault.

Switch A and Switch C are connected to the uplink network in link aggregation mode. When all uplink interfaces of Switch A and Switch C fails, Switch B needs to sense fault in time switches traffic to the standby link. Therefore, you should deploy failover on Switch A and Switch C.

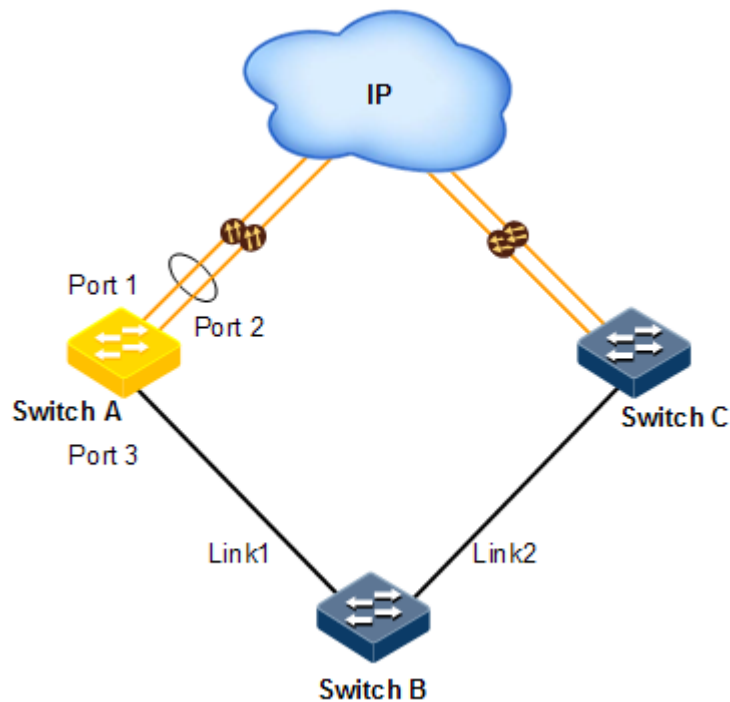


Figure 7-6 Configuring failover

Configuration steps

Step 1 Configure failover on Switch A.

Create the failover group.

```
Alpha-A28E#config  
Alpha-A28E(config)#link-state-tracking group 1
```

Add uplink interfaces to the failover group.

```
Alpha-A28E(config)#interface port 1  
Alpha-A28E(config-port)#link-state-tracking group 1 upstream
```

```
Alpha-A28E(config-port)#exit
Alpha-A28E(config)#interface port 2
Alpha-A28E(config-port)#link-state-tracking group 1 upstream
Alpha-A28E(config-port)#exit
```

Add downlink interfaces to the failover group.

```
Alpha-A28E(config)#interface port 3
Alpha-A28E(config-port)#link-state-tracking group 1 downstream
```

Step 2 Configure failover on Switch C.

Configurations are identical to the ones on Switch A.

Checking results

This guide takes configurations on Switch A for an example.

Show failover group configurations by the command of **show link-state-tracking group**.

```
SwitchA#show link-state-tracking group 1
Link State Tracking Group: 1 (Enable)
Status: Normal
Fault type: None
Upstream Mep: --
Upstream Interfaces:
  Port 1(Up) Port 2(Up)
Downstream Interfaces:
  Port 3(Up)
```

After all uplinks of Switch A fails, show failover group configurations by the command of **show link-state-tracking group**. In this case, you can learn that downlink Port 3 is disabled.

```
SwitchA#show link-state-tracking group 1
Link State Tracking Group: 1 (Enable)
Status: Failover
Fault type: Port-down
Upstream Mep: --
Upstream Interfaces:
  Port 1(Down) Port 2(Down)
Downstream Interfaces:
  Port 3(Disable)
```

7.4 STP

7.4.1 Introduction

STP

With the increasing complexity of network structure and growing number of switches in the network, the Ethernet network loops become the most prominent problem. Because of the packet broadcast mechanism, network loop will make the network generate network storm, exhaust network resources, and have serious impact to the normal data forwarding. The network storm caused by network loops is shown as below.

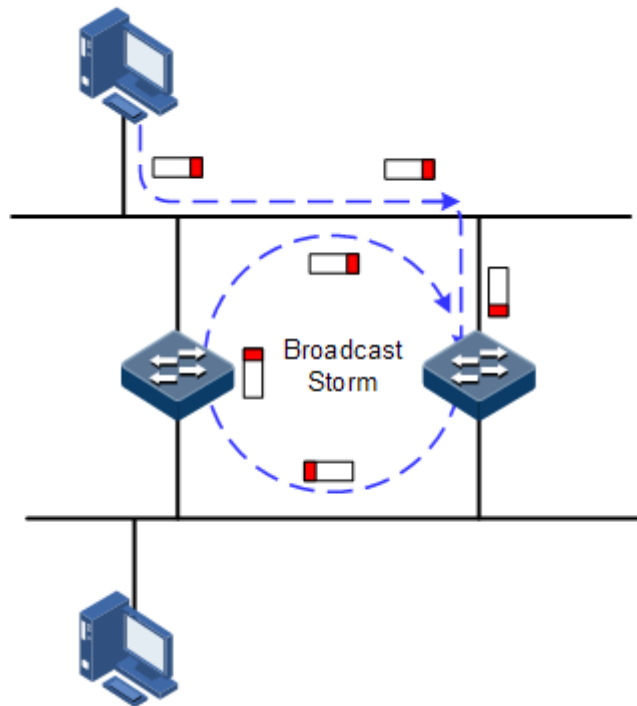


Figure 7-7 Network storm due to loopback

Spanning Tree Protocol (STP) is compliant to IEEE 802.1d standard and used to remove data physical loop in data link layer in LAN.

The A10E/A28E running STP can process Bridge Protocol Data Unit (BPDU) packet with each other for the election of root switch and selection of root port and designated port. It also can block loop interface on the A10E/A28E logically according to the selection results, eventually trimming the loop network structure to tree network structure without loop which takes a A10E/A28E as root, so as to prevent the continuous proliferation and limitless circulation of packet in loop network from causing broadcast storm and avoid declining packet processing capacity caused by receiving the same packets repeatedly.

The loop network diagram running STP is shown as below.

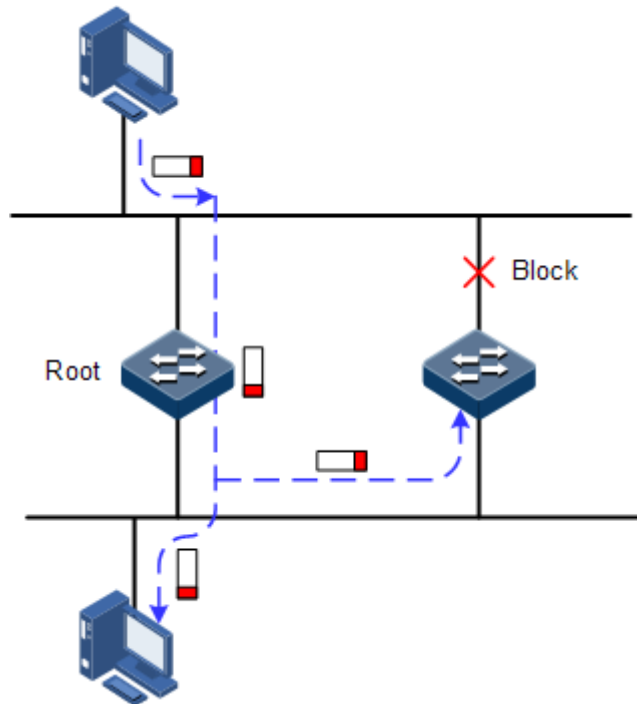


Figure 7-8 Loop networking with STP

Although STP can eliminate loop network and prevent broadcast storm well, its shortcomings are still gradually exposed with thorough application and development of network technology.

The major disadvantage of STP is the slow convergence speed.

RSTP

For improving the slow convergent speed of STP, IEEE 802.1w establishes Rapid Spanning Tree Protocol (RSTP), which increases the mechanism to change interface blocking state to forwarding state, speed up the topology convergence rate.

The purpose of STP/RSTP is to simplify a bridge connection LAN to a unitary spanning tree in logical topology and so as to avoid broadcast storm.

The disadvantages of STP/RSTP are exposed with the rapid development of VLAN technology. The unitary spanning tree simplified from STP/RSTP leads the below problems:

- The whole switched network has only one spanning tree, which will lead to longer convergence time in a larger network.
- Waste of bandwidth since a link does not carry any flow after it is blocked;
- Packet of partial VLAN cannot be forwarded when network structure is unsymmetrical. As shown below, Switch B is the root switch, RSTP blocks the link between Switch A and Switch C logically and makes that the VLAN 100 packet cannot be transmitted and Switch A and Switch C cannot communicate.

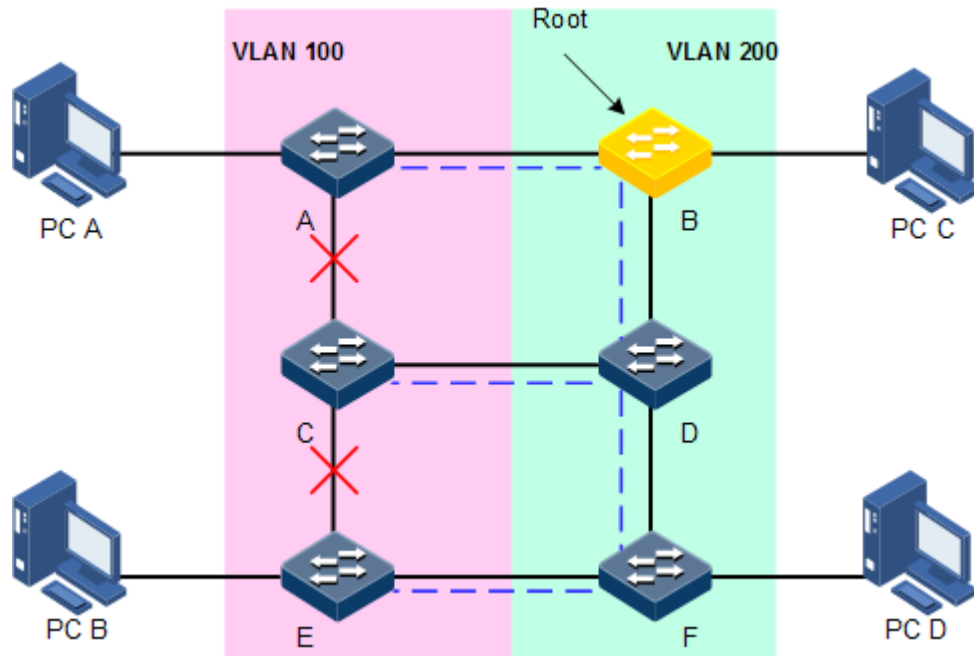


Figure 7-9 VLAN packet forward failure due to RSTP

7.4.2 Preparation for configuration

Networking situation

In big LAN, multiple devices are concatenated for inter-access among hosts. They need to enable STP to avoid loop among the devices, MAC address learning fault, and broadcast storm and network down caused by quick copy and transmission of data frame. STP calculation can block one interface in a broken loop and make sure that there is only one path from data flow to destination host, which is also the best path.

Preconditions

Configure interface physical parameters to make it Up before configuring STP.

7.4.3 Default configurations of STP

The default configuration of STP is as below.

Function	Default value
Global STP function status	Disable
Interface STP function status	Enable
STP priority of device	32768
STP priority of interface	128
Interface path cost	0
max-age timer	20s

Function	Default value
hello-time timer	2s
forward-delay timer	15s

7.4.4 Enabling STP

Configure STP on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# spanning-tree enable	Enable STP.

7.4.5 Configuring STP parameters

Configure STP enable for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# spanning-tree priority <i>priority-value</i>	(Optional) configure device priority.
3	Alpha-A28E(config)# spanning-tree root { primary secondary }	(Optional) configure the A10E/A28E as the root or backup device.
4	Alpha-A28E(config)# interface port <i>port-id</i> Alpha-A28E(config-port)# spanning-tree priority <i>priority-value</i>	(Optional) configure device interface priority.
5	Alpha-A28E(config-port)# spanning-tree inter-path-cost <i>cost-value</i> Alpha-A28E(config-port)# exit	(Optional) configure interface path cost.
6	Alpha-A28E(config)# spanning-tree hello-time <i>value</i>	(Optional) configure Hello Time.
7	Alpha-A28E(config)# spanning-tree transit-limit <i>value</i>	(Optional) configure maximum transmitting speed of interface.
8	Alpha-A28E(config)# spanning-tree forward-delay <i>value</i>	(Optional) configure forward delay.
9	Alpha-A28E(config)# spanning-tree max-age <i>value</i>	(Optional) configure maximum age.

7.4.6 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show spanning-tree [detail]	Show basic configuration information of STP.
2	Alpha-A28E# show spanning-tree port-list <i>port-list</i> [detail]	Show STP configuration on the interface.

7.4.7 Example for configuring STP

Networking requirements

As shown below, Switch A, Switch B, and Switch C forms a ring network, so the loopback problem must be solved in the situation of a physical ring. Enable STP on them, set the priority of Switch A to 0, and path cost from Switch B to Switch A to 10.

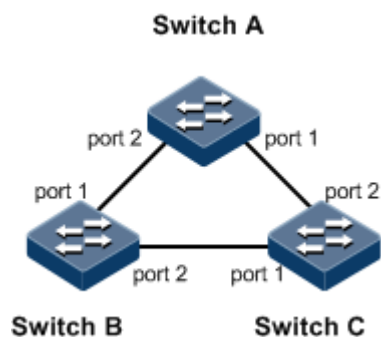


Figure 7-10 STP application networking

Configuration steps

Step 1 Enable STP on Switch A, Switch B, and Switch C.

Configure Switch A.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree mode stp
```

Configure Switch B.

```
Alpha-A28E#hostname SwitchB
SwitchB#config
```

```
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree mode stp
```

Configure Switch C.

```
Alpha-A28E#hostname SwitchC
SwitchC#config
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree mode stp
```

Step 2 Configure interface mode on three switches.

Configure Switch A.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
```

Configure Switch C.

```
SwitchC(config)#interface port 1
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
SwitchC(config)#interface port 2
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
```

Step 3 Configure priority of spanning tree and interface path cost.

Configure Switch A.


```
SwitchA(config)#spanning-tree priority 0
SwitchA(config)#interface port 2
SwitchA(config-port)#spanning-tree inter-path-cost 10
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#spanning-tree inter-path-cost 10
```

Checking results

Use the **show spanning-tree** command to view bridge status. Take Switch A for example.

```
SwitchA#show spanning-tree
Spanning-tree Admin State: enable
Spanning-tree protocol Mode: STP
BridgeId:    Mac 000E.5E7B.C557 Priority 0
Root:        Mac 000E.5E7B.C557 Priority 0 RootCost 0
Operational: HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:  HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
```

Use the **show spanning-tree port-list** *port-list* command to view interface status. Take Switch A for example.

```
SwitchA#show spanning-tree port-list 1,2
Port1
PortEnable: admin: enable oper: enable
Rootguard: disable
Loopguard: disable
ExternPathCost:10
EdgedPort: admin: auto oper: no BPDU Filter: disable
LinkType: admin: auto oper: point-to-point
Partner STP Mode: stp
Bpdu send: 279 (TCN<0> Config<279> RST<0> MST<0>)
Bpdu received:13 (TCN<13> Config<0> RST<0> MST<0>)
Instance PortState PortRole PortCost(admin/oper) PortPriority
-----
0 discarding disabled 200000/200000 0

Port2
PortEnable: admin: enable oper: enable
Rootguard: disable
Loopguard: disable
ExternPathCost:200000
EdgedPort: admin: auto oper: no BPDU Filter: disable
LinkType: admin: auto oper: point-to-point
Partner STP Mode: stp
```

```
Bpdus send: 279 (TCN<0> Config<279> RST<0> MST<0>)
Bpdus received:6 (TCN<6> Config<0> RST<0> MST<0>)
Instance PortState PortRole PortCost(admin/oper) PortPriority
-----
0 discarding disabled 10/10 0
```

7.5 MSTP

7.5.1 Introduction

Multiple Spanning Tree Protocol (MSTP) is defined by IEEE 802.1s. Recovering the disadvantages of STP and RSTP, the MSTP realizes fast convergence and distributes different VLAN flow following its own path to provide an excellent load sharing mechanism.

MSTP divides a switch network into multiple domains, called MST domain. Each MST domain contains several spanning trees but the trees are independent one another. Each spanning tree is called a Multiple Spanning Tree Instance (MSTI).

MSTP protocol introduces Common Spanning Tree (CST) and Internal Spanning Tree (IST) concepts. CST refers to take MST domain as a whole to calculate and generate a spanning tree. IST means to generate spanning tree in internal MST domain.

Compared with STP and RSTP, MSTP also introduces total root (CIST Root) and domain root (MST Region Root) concepts. The total root is a global concept; all switches running STP/RSTP/MSTP can only have one total root, which is the CIST Root. The domain root is a local concept, which is relative to an instance in a domain. As shown below, all connected devices only have one total root, and the number of domain root contained in each domain is associated with the number of instances.

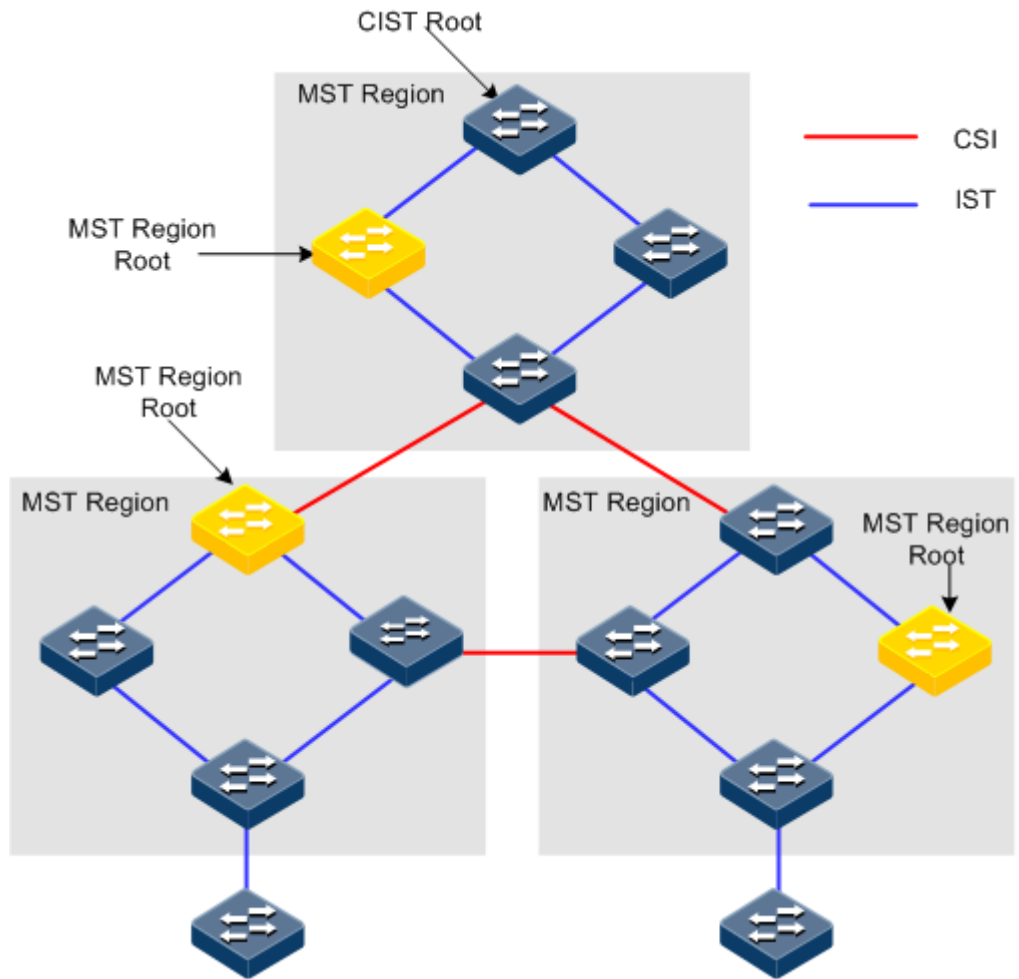


Figure 7-11 Basic concepts of the MSTI network

There can be different MST instance in each MST domain, which associates VLAN and MSTI by setting VLAN mapping table (relationship table of VLAN and MSTI). The concept sketch map of MSTI is shown as below.

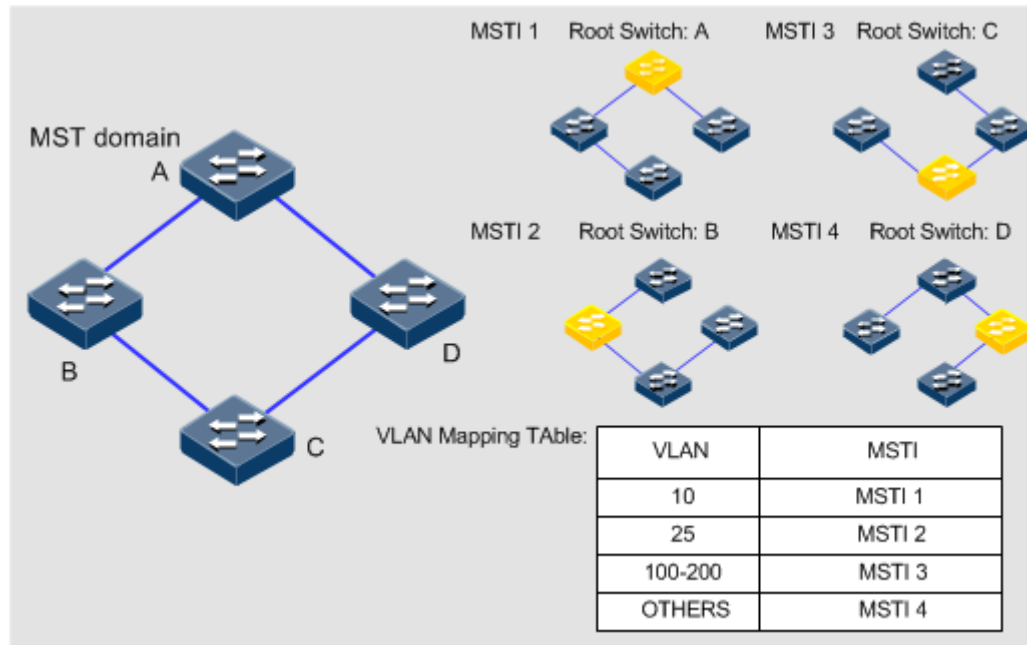


Figure 7-12 MSTI concepts



Note

Each VLAN can map to one MSTI; that is to say, data of one VLAN can only be transmitted in one MSTI while one MSTI may correspond to several VLAN.

Compared with the previous STP and RSTP, MSTP has obvious advantages, including cognitive ability of VLAN, load balance sharing ability, similar RSTP port status switching ability as well as binding multiple VLAN to one MST instance to reduce resource occupancy rate. In addition, MSTP running devices in network are also compatible with the devices running STP and RSTP.

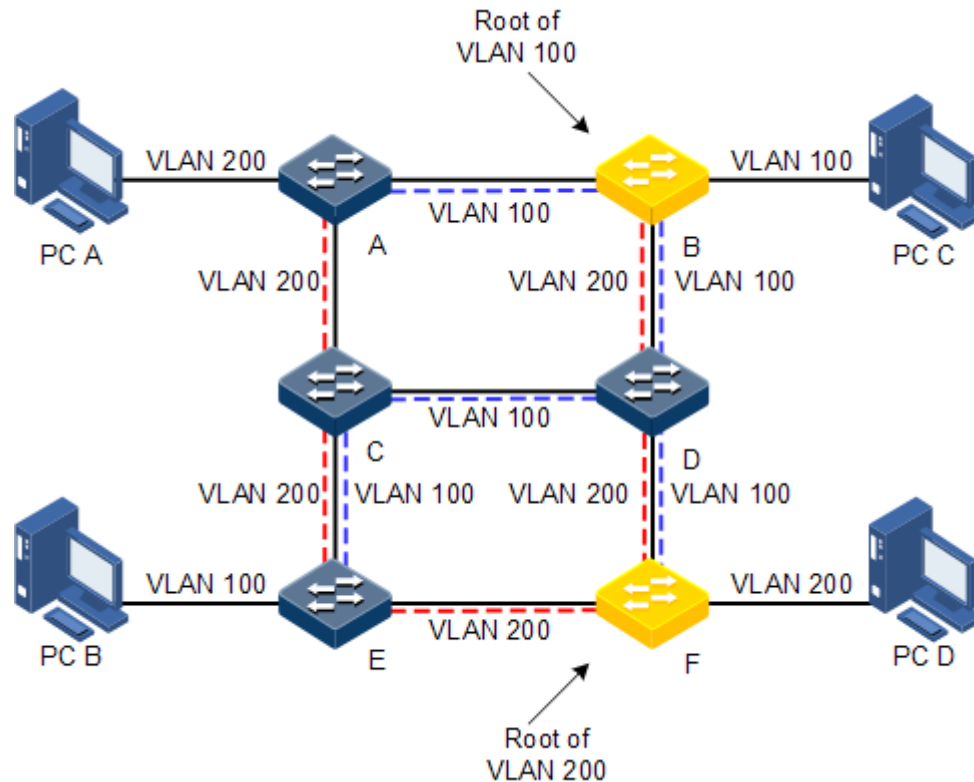


Figure 7-13 Networking of multiple spanning trees instances in MST domain

Applying MSTP in the network as Figure 3-10 above, after calculation, there are two spanning trees generated at last (two MST instances):

- MSTI1 takes Switch B as the root switch, forwarding packet of VLAN100.
- MSTI2 takes Switch F as the root switch, forwarding packet of VLAN200.

In this way, all VLANs can communicate at internal, different VLAN packets are forwarded in different paths to share loading.

7.5.2 Preparation for configuration

Scenario

In big LAN or residential region aggregation, the aggregation devices will make up a ring for link backup, at the same time avoid loop and realize service load sharing. MSTP can select different and unique forwarding path for each one or a group of VLAN.

Prerequisite

Configure interface physical parameters to make it Up before configuring MSTP.

7.5.3 Default configurations of MSTP

The default configuration of MSTP is as below.

Function	Default value
Global MSTP function status	Disable
Interface MSTP function status	Enable
Maximum hop count of MST domain	20
MSTP priority of device	32768
MSTP priority of interface	128
Path cost of interface	0
Maximum number of packets sent within each Hello time	3
Max Age timer	20s
Hello Time timer	2s
Forward Delay timer	15s
Revision level of MST domain	0

7.5.4 Enable MSTP

Configure MSTP for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# spanning-tree enable	Enable global STP.

7.5.5 Configuring MST domain and its maximum hop count

You can set domain information for the A10E/A28E when it is running in MSTP mode. The device MST domain is decided by domain name, VLAN mapping table and configuration of MSTP revision level. You can set current device in a specific MST domain through following configuration.

MST domain scale is restricted by the maximum hop count. Starting from the root bridge of spanning tree in the domain, the configuration message (BPDU) reduces 1 hop count once it is forwarded passing a device; the A10E/A28E discards the configuration message with hop count 0. The device out of maximum hop count cannot join spanning tree calculation and then restrict MST domain scale.

Configure MSTP domain and its maximum hop count for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# spanning-tree region-configuration	Enter MST domain configuration mode.

Step	Configuration	Description
3	Alpha-A28E(config-region)# name <i>name</i>	Configure MST domain name.
4	Alpha-A28E(config-region)# revision-level <i>level-value</i>	Set revision level for MST domain.
5	Alpha-A28E(config-region)# instance <i>instance-id</i> vlan <i>vlan-list</i> Alpha-A28E(config-region)# exit	Set mapping relationship from MST domain VLAN to instance.
6	Alpha-A28E(config)# spanning-tree max-hops <i>hops-value</i>	Configure the maximum hop count for MST domain.



Note

The maximum hop count is MST domain maximum hop count if and only if the configured device is root of the domain; other roots cannot configure this item effectively.

7.5.6 Configuring root bridge/backup bridge

Two methods for MSTP root selection: one is to configure device priority and calculated by STP to confirm the STP root bridge or backup bridge; the other is to assign MSTP root directly by this command. When the root bridge has fault or power off, the backup bridge can take the place of the root bridge for related instance. In this cast, if user has set new root bridge, the backup bridge will not become the root bridge. If user has configured several backup bridges for a spanning tree, once the root bridge stops working, MSTP will choose the backup root with the smallest MAC address as new root bridge.



Caution

It is recommended that you not modify the priority of any device in the network if adopting direct assigning root bridge method, otherwise, the assigned root bridge or backup bridge may be invalid.

Configure root bridge or backup bridge for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# spanning-tree [instance <i>instance-id</i>] root { primary secondary }	Set the A10E/A28E as root bridge or backup bridge for a STP instance.



Note

- You can confirm the effective instance of the root bridge or backup bridge through the parameter **instance** *instance-id*. The current device will be assigned as the

root bridge or backup bridge of CIST if instance-id is 0 or parameter **instance instance-id** is omitted.

- The roots in device instances are independent mutually, that is to say, they cannot only be the root bridge or backup bridge of one instance, but also the root bridge or backup bridge of other spanning tree instances. However, in the same spanning tree instance, the same device cannot be used as the root bridge and backup bridge at the same time.
- You cannot assign two or more root bridges for one spanning tree instance, but can assign several backup bridges for one spanning tree. Generally speaking, you had better assign one root bridge and several backup bridges for a spanning tree.

7.5.7 Configuring device interface and system priority

Whether the interface is selected as root interface can be judged by interface priority. Under the identical condition, the smaller priority interface will be selected as root interface. An interface may have different priorities and play different roles in different instances.

The device Bridge ID decides whether it can be selected as root of spanning tree. Configuring smaller priority helps get smaller device Bridge ID and designate the A10E/A28E as root. If priority is identical, the A10E/A28E with smaller MAC address will be selected as root.

Similar to configuring root and backup root, priority is independent mutually in different instances. You can confirm priority instance through parameter **instance instance-id**. Configure bridge priority for CIST if instance-id is 0 or parameter **instance instance-id** is omitted.

Configure interface priority and system priority for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# spanning-tree [instance instance-id] priority priority-value Alpha-A28E(config-port)# exit	Set interface priority for a STP instance.
4	Alpha-A28E(config)# spanning-tree [instance instance-id] priority priority-value	Set system priority for a STP instance.



Note

The value of priority must be multiples of 4096, like 0, 4096, 8192, etc. It is 32768 by default.

7.5.8 Configuring network diameter for switch network

Network diameter indicates the nodes number on the path has the most device number in switch network. In MSTP, network diameter is valid only to CIST, and invalid to MSTI instance. No matter how many nodes in a path in one domain, it is considered as just one node. Actually, network diameter should be defined as the domain number in the path crossing the most domains. The network diameter is 1 if there is only one domain in the whole network.

The maximum hop count of MST domain is used to restrict domain scale, while network diameter is a parameter to denote the whole network scale. The bigger the network diameter is, the bigger the network scale is.

Similar to the maximum hop count of MST domain, if and only if configuring the A10E/A28E as CIST root device, this configuration is effective. MSTP will automatically set Hello Time, Forward Delay and Max Age parameters to a privileged value by calculation when configuring network diameter.

Configure network diameter for switch network for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# spanning-tree bridge-diameter <i>bridge-diameter-value</i>	Configure diameter for switch network.

7.5.9 Configuring inner path overhead for interfaces

When selecting root port and designated port, the smaller the interface path cost is, the easier it is to be selected as root port or designated port. Inner path costs of interface are independently mutually in different instances. You can configure inner path cost for instance through parameter **instance** *instance-id*. Configure inner path cost of interface for CIST if instance-id is 0 or parameter **instance** *instance-id* is omitted.

By default, interface cost often depends on the physical features:

- 10 Mbit/s: 2000000
- 100 Mbit/s: 200000
- 1000 Mbit/s: 20000
- 10 Gbit/s: 2000

Configure inner path cost for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# spanning-tree [instance <i>instance-id</i>] inter-path-cost <i>cost-value</i>	Configure inner path cost for interface.

7.5.10 Configuring external path cost for interface

External path cost is the cost from the device to CIST root, which is equal in the same domain.

Configure external path cost for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config- port)# spanning-tree extern-path-cost <i>cost-value</i>	Configure external path cost for interface.

7.5.11 Configuring maximum transmitting speed for interface

Interface maximum transmitting speed means MSTP permitted transmitting maximum BPDU number in each Hello Time. This parameter is a relative value and no unit. The bigger the parameter is configured, the more packets are permitted to transmit in a Hello Time, the more device resource it takes up. The same to time parameter, only root device configuration is valid.

Configure interface maximum transmitting speed for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# spanning-tree transit-limit <i>value</i>	Configure interface maximum transmitting speed.

7.5.12 Configuring MSTP timer

- Hello Time: the A10E/A28E sends the time interval of bridge configuration information (BPDU) regularly to check whether there is failure in detection link of device. The A10E/A28E sends hello packets to other devices around in Hello Time to check if there is fault in the link. The default value is 2 seconds, and user can adjust the interval value according to network condition. Reduce the interval when network link changes frequently to enhance the stability of STP; by contrary, increasing interval value will reduce system CPU resource occupation rate for STP.
- Forward Delay: time parameter to ensure the safe remove of device status. Link fault leads to network re-calculate spanning tree, but the new configuration message recalculated cannot be transmitted to the whole network immediately. There may be temporary loop if the new root port and designated port start transmitting data at once. This protocol adopts status remove system: before root port and designated interface starting data forwarding, it needs a medium status (learning status), after delay for the interval of Forward Delay, it enters forwarding status. The delay guarantees the new configuration message to be transmitted through whole network. You can adjust the delay value according to real condition, reduce it when network topology changes infrequently and increase it in opposite.
- Max Age: the bridge configuration information used by STP has a life time that is used to judge whether the configuration information is outdated. The A10E/A28E will discard outdated information and STP will recalculate spanning tree. The default value is 20 seconds. Too small age value may cause the frequent re-calculation of spanning tree, while too bigger age value will make STP not adapt network topology change timely.

All devices in the whole switch network adopt the three time parameters on CIST root device, so only the root device configuration is valid.

Configure timer for the A10E/A28E as below.

Step	Configuration	Description
1	<code>Alpha-A28E#config</code>	Enter global configuration mode.
2	<code>Alpha-A28E(config)#spanning-tree hello-time value</code>	Set Hello Time.
3	<code>Alpha-A28E(config)#spanning-tree forward-delay value</code>	Set Forward Delay.
4	<code>Alpha-A28E(config)#spanning-tree max-age value</code>	Set Max Age.

7.5.13 Configuring edge interface

The edge interface indicates the interface neither direct connects to any devices nor indirect connect to any device via network.

The edge port can change the interface status to forward quickly without any waiting time. You had better set the Ethernet interface connected to user client as edge port to make it quick to change to forward status.

The edge interface attribute depends on actual condition when it is in auto-detection mode; the real port will change to false edge interface after receiving BPDU when it is in force-true mode; when the interface is in force-false mode, whether it is true or false edge port in real operation, it will maintain the force-false mode until the configuration is changed.

By default, all interfaces on the A10E/A28E are set in auto-detection attribute.

Configure the edge interface for the A10E/A28E as below.

Step	Configuration	Description
1	<code>Alpha-A28E#config</code>	Enter global configuration mode.
2	<code>Alpha-A28E(config)#interface port port-id</code>	Enter physical layer interface configuration mode.
3	<code>Alpha-A28E(config-port)#spanning-tree edged-port { auto force-true force-false }</code>	Configure RSTP edge port attributes.

7.5.14 Configuring STP/MSTP mode switching

When STP is enabled, three spanning tree modes are supported as below:

- STP compatible mode: the A10E/A28E does not implement fast switching from the replacement interface to the root interface and fast forwarding by a specified interface; instead it sends STP configuration BPDU and STP Topology Change Notification (TCN) BPDU. After receiving MST BPDU, it discards unidentifiable part.

- MSTP mode: the A10E/A28E sends MST BPDU. If the peer device runs STP, the local interface is switched to STP compatible mode. If the peer device runs MSTP, the local interface remains in RSTP mode, and process packets as external information of domain.

Configure the A10E/A28E as below.

Step	Configuration	Description
1	A1pha-A28E# config	Enter global configuration mode.
2	A1pha-A28E(config)# spanning-tree mode { stp rstp mstp }	Configure spanning tree mode.

7.5.15 Configuring link type

The point-to-point link connected interface can quickly changes to forward status by transmitting synchronization packet. By default, MSTP set interface link type according to duplex mode. Full-duplex interface is considered as point-to-point link, half-duplex interface is considered as shared link.

You can configure current Ethernet interface to connect point-to-point link by force, but it will go wrong if the link is not point-to-point. Generally, user had better set this item in auto status and the system will automatically detect whether the interface is connected to point-to-point link.

Configure link type for the A10E/A28E as below.

Step	Configuration	Description
1	A1pha-A28E# config	Enter global configuration mode.
2	A1pha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	A1pha-A28E(config-port)# spanning-tree link-type { auto point-to-point shared }	Configure link type for interface.

7.5.16 Configuring root interface protection

Network will select bridge again when it receives packet from higher priority, which will influent network connectivity and also consume CPU resource. For MSTP network, if someone sends higher priority BPDU packets, the network may become unstable for the continuous election. Generally, each bridge priority has already configured in network programming. The nearer to edge, the lower the bridge priority is. So the down-bound interface cannot receive the packets higher than bridge priority only if someone attacks. For these interfaces, user can enable rootguard function to refuse to deal with packet higher than bridge priority and meanwhile block the interface for a period to prevent other attacks from attack source to damage the upper layer link.

Configure root interface protection for the A10E/A28E as below.

Step	Configuration	Description
1	A1pha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# spanning-tree rootguard { enable disable }	Configure root interface protection.

7.5.17 Configuring interface loopguard

The spanning tree has two functions: loopguard and link backup. Loopguard requires carving up topology network into tree structure. There must be redundant link in topology if requiring link backup. Spanning tree can avoid loop by blocking the redundant link and enable link backup function by opening redundant link when the link breaks down.

Spanning tree module exchanges packets periodically, and the link has failed if it has not received packet in a period. Then select a new link and enable backup interface. In actual network application, the packet cannot be received not only for link fault, then at this time, enable backup interface may lead to loop link.

Purpose of loopguard is to keep the original interface status when it cannot receive packet in a period.

Loopguard and link backup functions are exclusive, loopguard requires disabling link backup to avoid loop.

Configure interface loop protection for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# spanning-tree loopguard { enable disable }	Configure interface loopguard attributes.

7.5.18 Executing mcheck operation

Interface on MSTP device has two working modes: STP compatible mode and MSTP mode. Suppose the interface of MSTP device in a switch network is connected to the A10E/A28E running STP, the interface will change to work in STP compatible mode automatically. But the interface cannot change to work in MSTP mode if the A10E/A28E running STP is removed, i.e. the interface still works in STP compatible mode. You can execute the **mcheck** command to force the interface working in MSTP mode. If the interface receives new STP packet again, it will return to STP compatible mode.

Configure the A10E/A28E to execute mcheck operation as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# spanning-tree mcheck	Execute mcheck operation, force to remove interface to MSTP mode.

7.5.19 Checking configuration

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show spanning-tree	Show basic configurations of STP.
2	Alpha-A28E# show spanning-tree [<i>instance instance-id</i>] port- list port-list [<i>detail</i>]	Show configurations of spanning tree on the interface.
3	Alpha-A28E# show spanning-tree region-operation	Show MST domain operation information.
4	Alpha-A28E(config-region)# show spanning-tree region-configuration	Show MST domain configuration information.

7.5.20 Maintenance

Maintain the A10E/A28E as below.

No.	Command	Description
1	Alpha-A28E(config-port)# spanning-tree clear statistics	Clear statistics of spanning tree on the interface.

7.5.21 Example for configuring MSTP

Networking requirements

As shown below, three A10E/A28E devices are connected to form a ring network through MSTP, with the domain name aaa. Switch B, connected with a PC, belongs to VLAN 3. Switch C, connected with another PC, belongs to VLAN 4. Instance 3 is related to VLAN 3. Instance 4 is related to VLAN 4. Configure the path cost of instance 3 on Switch B so that packets of VLAN 3 and VLAN 4 are forwarded respectively in two paths, which eliminates loopback and implements load balancing.

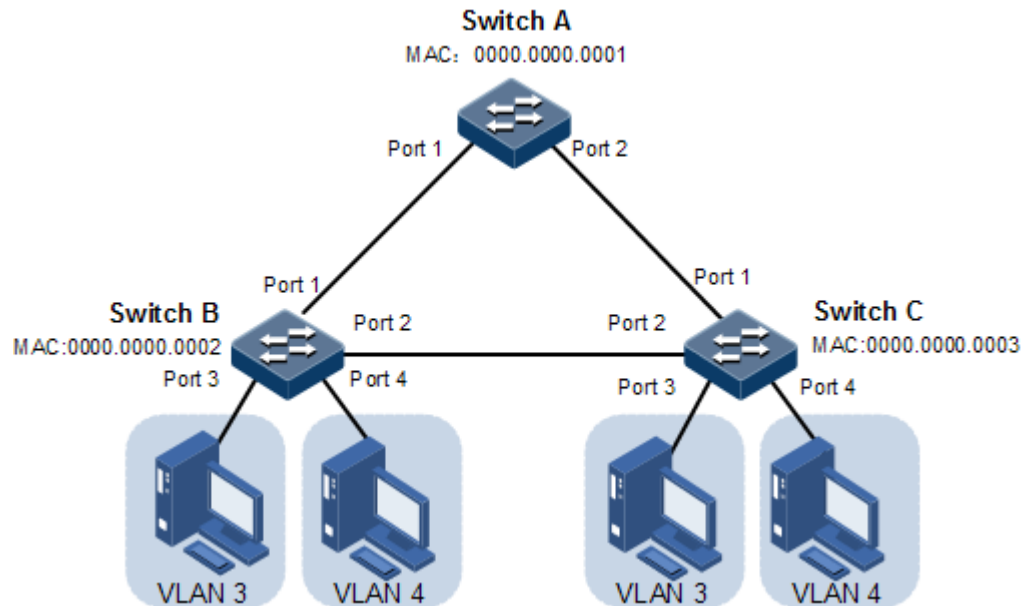


Figure 7-14 MSTP application networking

Configuration steps

- Step 1 Create VLAN 3 and VLAN 4 on Switch A, Switch B, and switch C respectively, and activate them.

Configure Switch A.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 3-4 active
```

Configure Switch B.

```
Alpha-A28E#hostname SwitchB
SwitchB#config
SwitchB(config)#create vlan 3-4 active
```

Configure Switch C.

```
Alpha-A28E#hostname SwitchC
SwitchC#config
SwitchC(config)#create vlan 3-4 active
```

- Step 2 Configure Port 1 and Port 2 of Switch A to allow all VLAN packets to pass in Trunk mode. Configure Port 1 and Port 2 of Switch B to allow all VLAN packets to pass in Trunk mode.

Configure Port 1 and Port 2 of Switch C to allow all VLAN packets to pass in Trunk mode. Configure Port 3 and Port 4 of Switch B and Switch C to allow packets of VLAN 3 and VLAN 4 to pass in Access mode.

Configure Switch A.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport access vlan 3
SwitchB(config-port)#exit
SwitchB(config)#interface port 4
SwitchB(config-port)#switchport access vlan 4
SwitchB(config-port)#exit
```

Configure Switch C.

```
SwitchC(config)#interface port 1
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
SwitchC(config)#interface port 2
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
SwitchC(config)#interface port 3
SwitchC(config-port)#switchport access vlan 3
SwitchC(config-port)#exit
SwitchC(config)#interface port 4
SwitchC(config-port)#switchport access vlan 4
SwitchC(config-port)#exit
```

- Step 3 Set spanning tree mode of Switch A, Switch B, and Switch C to MSTP, and enable STP. Enter MSTP configuration mode, and set the domain name to aaa, revised version to 0. Map instance 3 to VLAN 3, and instance 4 to VLAN 4. Exit from MST configuration mode.

Configure Switch A.


```
SwitchA(config)#spanning-tree mode mstp
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree region-configuration
SwitchA(config-region)#name aaa
SwitchA(config-region)#revision-level 0
SwitchA(config-region)#instance 3 vlan 3
SwitchA(config-region)#instance 4 vlan 4
```

Configure Switch B.

```
SwitchB(config)#spanning-tree mode mstp
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree region-configuration
SwitchB(config-region)#name aaa
SwitchB(config-region)#revision-level 0
SwitchB(config-region)#instance 3 vlan 3
SwitchB(config-region)#instance 4 vlan 4
SwitchB(config-region)#exit
```

Configure Switch C.

```
SwitchC(config)#spanning-tree mode mstp
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree region-configuration
SwitchC(config-region)#name aaa
SwitchC(config-region)#revision-level 0
SwitchC(config-region)#instance 3 vlan 3
SwitchC(config-region)#instance 4 vlan 4
```

Step 4 Set the inner path coast of Port 2 of spanning tree instance 3 to 500000 on Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#spanning-tree instance 3 inter-path-cost 500000
```

Checking result

Use the **show spanning-tree region-operation** command to show configurations of the MST domain.

```
Alpha-A28E#show spanning-tree region-operation
Operational Information:
-----
Name: aaa
Revision level: 0
```

```
Instances running: 3
Digest: 0X7D28E66FDC1C693C1CC1F6B61C1431C4
Instance      Vlans Mapped
-----
0             1,2,5-4094
3             3
4             4
```

Use the **show spanning-tree instance 3** command to check whether basic information about spanning tree instance 3 is correct.

- Switch A

```
SwitchA#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 3
-----
BridgeId:      Mac 0000.0000.0001 Priority 32768
RegionalRoot: Mac 0000.0000.0001 Priority 32768 InternalRootCost 0
PortId PortState PortRole PathCost PortPriority LinkType TrunkPort
-----
1       forwarding designated 200000 128          point-to-point no
2       forwarding designated 200000 128          point-to-point no
```

- Switch B

```
SwitchB#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 3
-----
BridgeId:      Mac 0000.0000.0002 Priority 32768
RegionalRoot: Mac 0000.0000.0001 Priority 32768 InternalRootCost
500000
PortId PortState PortRole PathCost PortPriority LinkType TrunkPort
-----
1       discarding alternate 500000 128          point-to-point no
3       forwarding root      200000 128          point-to-point no
...
```

- Switch C

```
SwitchC#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 3
-----
```

```
BridgeId:   Mac 0000.0000.0003 Priority 32768
RegionalRoot: Mac 0000.0000.0001 Priority 32768 InternalRootCost
200000
PortId PortState PortRole PathCost PortPriority LinkType TrunkPort
-----
2 forwarding root 200000 128 point-to-point no
3 forwarding designated 200000 128 point-to-point no
...
```

Use the **show spanning-tree instance 4** command to check whether basic information about spanning tree instance 4 is correct.

- Switch A

```
SwitchA#show spanning-tree instance 4
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 4
-----
BridgeId:   Mac 000E.5E00.0000 Priority 32768
RegionalRoot: Mac 000E.5E00.0000 Priority 32768 InternalRootCost 0
Port PortState PortRole PathCost PortPriority LinkType TrunkPort
-----
1 discarding disabled 200000 128 point-to-point yes
2 disabled disabled 200000 128 point-to-point yes
...
```

- Switch B

```
SwitchB#show spanning-tree instance 4
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 4
-----
BridgeId:   Mac 0000.0000.0002 Priority 32768
RegionalRoot: Mac 0000.0000.0001 Priority 32768 InternalRootCost
200000
PortId PortState PortRole PathCost PortPriority LinkType TrunkPort
-----
1 forwarding root 200000 128 point-to-point no
3 forwarding designated 200000 128 point-to-point no
...
```

- Switch C

```
SwitchC#show spanning-tree instance 4
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
```

```

MST ID: 4
-----
BridgeId:    Mac 0000.0000.0003 Priority 32768
RegionalRoot: Mac 0000.0000.0001 Priority 32768 InternalRootCost
200000
PortId  PortState  PortRole  PathCost  PortPriority  LinkType  TrunkPort
-----
2       forwarding  root      200000    128          point-to-point  no
3       discarding  alternate  200000    128          point-to-point  no
...

```

7.6 ERPS

7.6.1 Introduction

Ethernet Ring Protection Switching (ERPS) is an APS protocol over ITU-T G.8032 recommendation. It is specially used in Ethernet ring link protocol. Generally, ERPS can avoid broadcast storm caused by data loopback. When Ethernet has loop or device malfunction, ERPS can switch the link to backup link and ensure service restore quickly.

ERPS takes the control VLAN in ring network to transmit ring network control information and meanwhile, combining with the topology feature of ring network to discover network fault quickly and enable backup link to restore service fast.

7.6.2 Preparing for configurations

Scenario

With the development of Ethernet to telecom level network, voice and video multicast services bring forth higher requirements on Ethernet redundant protection and fault-restore time. The fault-restore convergent time of current STP system is in second level that is far away to meet requirement. ERPS can blocks a loop to avoid broadcast storm by defining different roles in the ring under normal situations. ERPS can switch the service link to backup link if the ring link or node faults and remove loop, perform fault protection switch and automatic fault restore, what's more, the protection switching time is lower than 50ms. It supports single ring, crossed rings and tangent rings networking modes.

ERPS supports fault detection in two modes:

- Fault detection based on physical interface status: to get link fault and switching quickly, available to neighbor devices
- Fault detection based on CFM: used in unidirectional fault detection or on multiple devices

Prerequisite

- Connect interface and configure physical parameters for it, the interface is Up at physical layer.
- Create VLAN, and add interfaces to the VLAN.

- CFM detection is configured between devices which are set to neighbor relations (for CFM mode).

7.6.3 Default configurations of ERPS

The default configuration of ERPS is as below.

Function	Default value
Protocol VLAN	1
Protection ring	Revertive mode
Protocol version	1
Ring WTR timer	5min
Ring protocol version	2
Guard timer	500ms
Ring HOLDOFF timer	0
ERPS fault information reported to network management system	Disable
Subring virtual path mode in intersecting node	with mode
Ring Propagate switch in intersecting node	Disable
Fault detection mode	Physical interface

7.6.4 Creating ERPS ring


Configure ERPS for the A10E/A28E as below.




Caution

- Only one device can be configured as the RPL (Ring Protection Link) Owner in a ring, and one device as the RPL Neighbour, other devices can only be configured as ring forwarding node.
- Tangent ring can be taken as two independent rings in fact, the configuration is identical to common single ring; intersecting rings has a master ring and a sub-ring, the configurations please refer to the section 7.6.5 (Optional) creating ERPS sub-ring.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# ethernet ring-protection <i>ring-id</i> east { port <i>port-id</i> port-channel <i>port-channel-number</i> } west { port <i>port-id</i> port-channel <i>port-channel-number</i> } [node-type <i>rpl-owner</i> <i>rpl</i> { east west }] [not-revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-list</i>]	<p>Create ring and configure node as RPL Owner.</p> <p>Protection ring changes to non-revertive mode if configured parameter of not-revertive. Flow switches back to current link from protection link after current link fault restore but it does not switch if in non-revertive mode.</p> <p> Note The east-bound and western-bound interface cannot be identical.</p>
	Alpha-A28E(config)# ethernet ring-protection <i>ring-id</i> east port <i>port-id</i> west port <i>port-id</i> node-type <i>rpl-neighbour</i> <i>rpl</i> { east west } [not-revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-list</i>]	Create ring and configure node as the RPL Neighbour.
	Alpha-A28E(config)# ethernet ring-protection <i>ring-id</i> east port <i>port-id</i> west port <i>port-id</i> [not-revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-list</i>]	Create ring and configure node as ring forwarding node.
3	Alpha-A28E(config)# ethernet ring-protection <i>ring-id</i> name <i>string</i>	(Optional) configure ring name. The length of name cannot exceed 32 strings.
4	Alpha-A28E(config)# ethernet ring-protection <i>ring-id</i> version { 1 2 }	(Optional) configure protocol version. All nodes in one ring must be consistent, version 1 differentiate ring via protocol VLAN, so different rings need configure different protocol VLAN, and so do version 2.
5	Alpha-A28E(config)# ethernet ring-protection <i>ring-id</i> guard-time <i>guard-time</i>	(Optional) during fault node restore time, after configuring Guard timer it does not deal with APS protocol packets. In some big ring network, restore node fault immediately may receive fault notice from neighbor node and cause link Down. Configure ring Guard timer can solve this problem.
6	Alpha-A28E(config)# ethernet ring-protection <i>ring-id</i> wtr-time <i>wtr-time</i>	(Optional) configure ring WTR timer. In revertive mode, waiting WTR timer timeout to switch back current link when current link restores from fault.

Step	Configuration	Description
7	Alpha-A28E(config)# ethernet ring-protection <i>ring-id</i> holdoff-time <i>holdoff-time</i>	(Optional) system delays fault report time when current link faults after configuring ring HOLDOFF timer. It can avoid current link switching frequently.  Note 50ms switching performance will be affected by HOLDOFF timer value if it is too bigger, so it is 0 by default.
8	Alpha-A28E(config)# ethernet ring-protection trap enable	(Optional) enable ERPS fault information report to NMS.


7.6.5 (Optional) creating ERPS sub-ring



Caution

- Only the intersecting rings network contains master ring and sub-ring.
- The master ring configuration is identical to the configuration of single ring or tangent ring. For details, see section 7.6.4 Creating ERPS ring.
- Un-crossed node on sub-ring is identical to configuration of single ring or tangent ring; see section 7.6.4 Creating ERPS ring for details.

Configure ERPS intersecting rings for A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ethernet ring-protection <i>ring-id</i> east { port <i>port-id</i> port-channel <i>port-channel-number</i> } west { port <i>port-id</i> port-channel <i>port-channel-number</i> } [node-type <i>rp</i>] owner <i>rp</i> { east west }] [not-revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-list</i>]	Create sub-ring and configure node as RPLOwner on crossover node. Protection ring changes to non-revertive mode if configured parameter of not-revertive. Flow switches back to current link from protection link after current link fault restore but it does not switch if in non-revertive mode.  Note The link between two crossover nodes in intersecting rings belongs to master ring, so either east-bound or wester-bound interface can be configured for sub-ring.

Step	Configuration	Description
	Alpha-A28E(config)# ethernet ring-protection ring-id east port port-id west port port-id node-type rpl-neighbour rpl { east west } [not-revertive] [protocol-vlan vlan-id] [block-vlanlist vlan-list]	Create sub-ring and configure node as RPLNeighbour on crossover nodes.
	Alpha-A28E(config)# ethernet ring-protection ring-id { east west } { port port-id port-channel port-channel-number } [not-revertive] [protocol-vlan vlan-id] [block-vlanlist vlan-list]	Create sub-ring and configure node as ring forwarding node on crossover nodes.
3	Alpha-A28E(config)# ethernet ring-protection ring-id raps-vc { with without }	(Optional) configure sub-ring virtual path mode on crossover node. Protocol packets transmitting in sub-ring is different from master ring, including with mode and without mode: <ul style="list-style-type: none"> • with: the primary ring transmits sub-ring protocol packets. • without: the sub-ring protocol VLAN transmits sub-ring protocol packets, so it cannot be included in the blocked VLAN list. <p>Configuration mode of two crossover nodes must be consistent.</p>
4	Alpha-A28E(config)# ethernet ring-protection ring-id propagate enable	Enable ring Propagate switch on crossover node. <p>Sub-ring data needs to be forwarded by master ring, so the sub-ring MAC address table also exists in master ring device. When sub-ring has fault, Propagate switch notifies master ring to refresh MAC address table in time and avoid flow lost.</p> <p>By default, disable Propagate switch. The command of ethernet ring-protection ring-id propagate disable can disable this function.</p>

7.6.6 Configuring ERPS fault detection

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ethernet ring-protection ring-id { east west } failure-detect physical-link	Configure physical interface fault detection mode.
	Alpha-A28E(config)# ethernet ring-protection ring-id { east west } failure-detect cc [md md-name] ma ma-name level level mep local-mep-id remote-mep-id	Configure CC fault detection mode. The fault detection mode will not take effect unless CFM is configured. MA must under md level if MD is configured.
	Alpha-A28E(config)# ethernet ring-protection ring-id { east west } failure-detect physical-link-or-cc [md md-name] ma ma-name level level mep local-mep-id remote-mep-id	Configure fault detection mode as physical interface or CC. Namely, the system reports fault either in physical link or CC mode. The fault detection mode will not take effect unless CFM is configured. MA must under md level if MD is configured.

7.6.7 (Optional) configuring ERPS switching control



Note

By default, flow will switch to protection link when current link is fault. Thus ERPS is needed in some special conditions.

Configure ERPS for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ethernet ring-protection ring-id force-switch { east west }	Configure forcible switching of ring flow to east or west.
3	Alpha-A28E(config)# ethernet ring-protection ring-id manual-switch { east west }	Configure forcible switching of ring flow to east or west. It has a lower priority than forcible switching or automatical switching upon fault of the current link.
4	Alpha-A28E(config)# clear ethernet ring-protection ring-id command	Clear switch control command, including force-switch and manual-switch.

7.6.8 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show ethernet ring-protection	Show ERPS ring configuration.
2	Alpha-A28E# show ethernet ring-protection status	Show ERPS ring status information.
3	Alpha-A28E# show ethernet ring-protection statistics	Show ERPS ring statistics.

7.6.9 Maintenance

You can maintain the A10E/A28E as below.

No.	Command	Description
1	Alpha-A28E(config)# clear ethernet ring-protection ring-id command	Clear the effect of ring switching control commands (force-switch and manual-switch)
2	Alpha-A28E(config)# clear ethernet ring-protection ring-id statistics	Clear protection ring statistic information.

7.7 RRPS

7.7.1 Introduction

With the development of Ethernet to the MAN, voice, video and multicast service has come up with higher requirements to the Ethernet redundancy protection and fault recovery time. The fault recovery convergence time of original STP mechanism is in the second level, which is far to meet the fault recovery time requirements of MAN.

RRPS solves the problems of weak protection to traditional data network and long time to fault recovery, which, in theory, can provide 50ms rapid protection features.

As shown below, blocked interface node is the master node, other nodes are transmission nodes. The master node generates by election. Each node can specify one loop interface as the first interface, the other as the second interface. The master node usually sends Hello packets periodically from the first interface and receives Hello packet sent by itself in the second interface under the circumstance of complete Ethernet ring. Then the master node will block the first interface immediately to ensure there is no loop when the ring network is in a complete state. For the other nodes on the RRPS, the first interface No. and the second interface No. play the same role basically.

RRPS generates master node by the election, so each node needs to collect device information on RRPS, only the right collection leads to correct election. Topology collection is completed

by Hello packets, which contain all nodes information the node collected from the other interface. The normal state of RRPS is shown below.

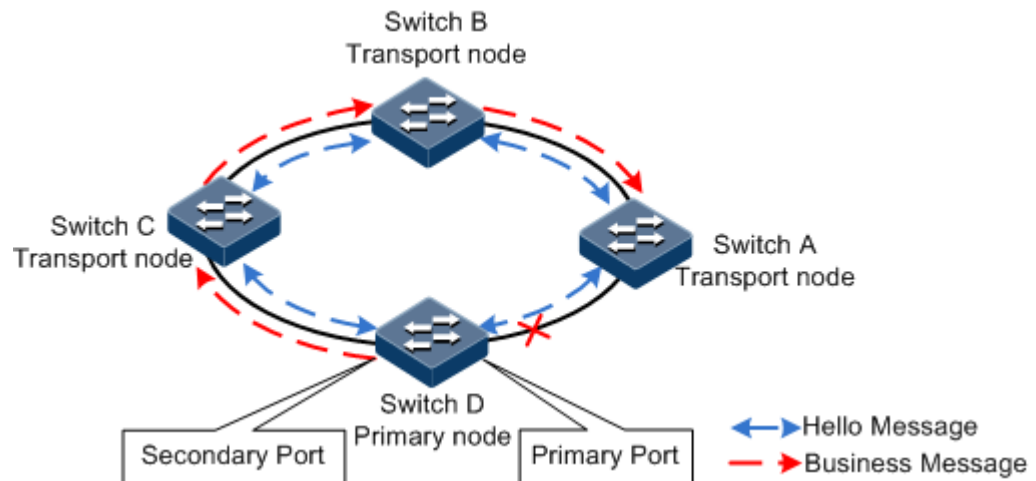


Figure 7-15 RRPS in normal status

According to the interface state of node ring, the ring node state can be divided into three types:

- Down: At least one of the two RRPS node interfaces is Down, then the node is Down.
- Block: At least one of the two RRPS node interfaces is Block, then the node is Block.
- Two-Forwarding: Both RRPS node interfaces are Forwarding, then the node is Two-Forwarding.

The election rules of master node are as follows:

- In all nodes on the ring, node with Down state is prior for master node, followed by Block and Two-Forward.
- If the nodes are in the same state, the node with high-priority Bridge is master node.
- If the nodes have the same state and priority, the node with large MAC address is master node.

Interface Block rules:

- All Link Down interfaces are Block.
- If the node is not master node, all Link Up ring interfaces are Forwarding.
- If the node is master node, then one of two interfaces is Block, the other is Forwarding. Rules are as follows:
 - Both interfaces are Up, the Block is the first interface;
 - If one interface is Down, then Block this interface.

The RRPS link failure is shown below.

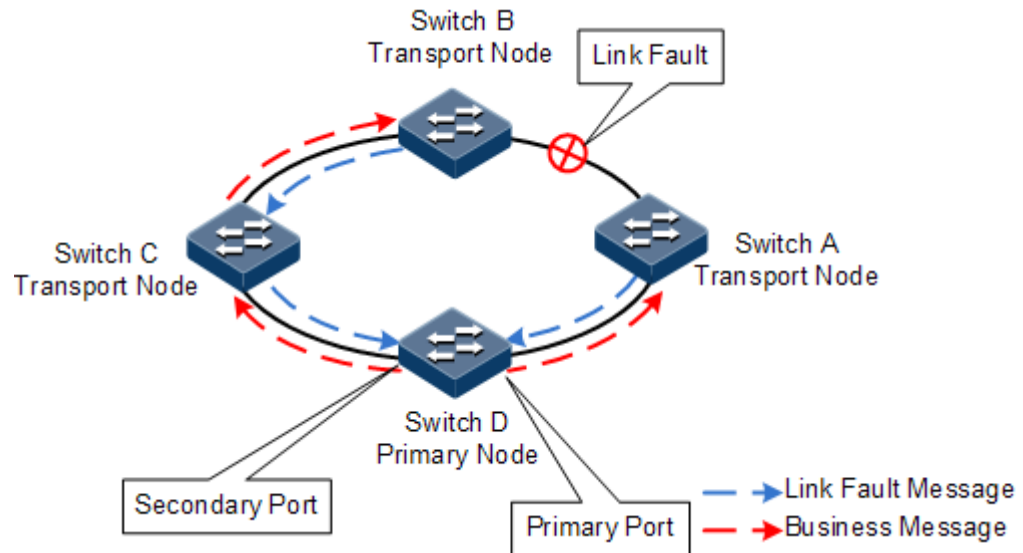


Figure 7-16 RRPS in switching status

Once there is link failure (such as link break), the failure adjacent node or interface will check the fault immediately and send link failure packets to master node. The master node will enable the first interface once receiving the packets, in the meantime, send packets to notify other transmission nodes about the link failure and inform them to change transmission direction. The data flow will be switched to normal link after the transmission nodes updating forwarding entry.

When the failed link is restored, the failed node does not enable the blocked port immediately until the new topology collection is stable. The origin node will find itself the master node, after some time delay, it will block his first interface, and send Change packets to notify the failed node enabling the blocked interface.

7.7.2 Preparing for configurations

Scenario

As a Metro Ethernet technology, Ethernet ring solves the problems of weak protection to traditional data network and long time to fault recovery, which, in theory, can provide 50ms rapid protection features and is compatible with traditional Ethernet protocol, is an important technology options and solutions of metro broadband access network optimization transformation.

RRPS technology is protocol, which through simple configuration achieves the elimination of ring loop, fault protection switching, and automatic fault recovery function and makes the fault protection switching time less than 50ms.

RRPS technology supports both single-ring and tangent ring networking modes, but not intersecting ring networking. Tangent ring is actually two separate single rings, which has the same configuration with common single ring.

Preconditions

Before configuring RRPS, configure interface physical parameters to make interface physical layer state Up.

7.7.3 Default configurations of RRPS

The default configuration of RRPS is as below.

Function	Default value
RRPS status	Disable
Hello packets transmitting time	1s
Fault recovery delay time	5s
RRPS description information	Ethernet ring X; X indicates RRPS ID.
Bridge priority	1
Ring interface aging time	15s
Ring protocol packets VLAN	2

7.7.4 Creating RRPS

Create a RRPS as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode. This interface is the first interface of ring node.
3	Alpha-A28E(config-port)# ethernet ring <i>ring-id secondary-interface-number</i>	Create ring and configure corresponding ring interface. This interface is the second interface of ring node.
4	Alpha-A28E(config-port)# exit Alpha-A28E(config)# ethernet ring <i>ring-id enable</i>	Enable Ethernet ring.


7.7.5 Configuring basic functions of RRPS



Caution

- For all devices in the same ring, suggest configure the fault recovery time, Hello packets interval. Ring protocol VLAN and Ring interface aging time separately for the same value.
- Interface aging time must be greater than twice of Hello time.

Configure the basic function of RRPS on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ethernet ring ring-id hello-time <i>hello-time</i>	(Optional) configure Hello packets transmitting time for RRPS.
3	Alpha-A28E(config)# ethernet ring ring-id restore-delay <i>delay-time</i>	(Optional) configure fault recovery delay time for RRPS. The link can be restored to the original current link until the recovery delay time timeout.
4	Alpha-A28E(config)# ethernet ring ring-id priority <i>priority</i>	(Optional) configure bridge priority for RRPS.
5	Alpha-A28E(config)# ethernet ring ring-id description <i>string</i>	(Optional) configure ring description information. It should be within 32 characters.
6	Alpha-A28E(config)# ethernet ring ring-id hold-time <i>hold-time</i>	(Optional) configure interface aging time for RRPS. If RRPS interface has not received Hello packets in aging time, age this interface and consider that the link circuit on link ring has fault. If the node interface is in Block state, it will enable the blocked interface temporarily to ensure the normal communication of all nodes on RRPS.
7	Alpha-A28E(config)# ethernet ring ring-id protocol-vlan <i>vlan-id</i>	(Optional) configure RRPS VLAN.
8	Alpha-A28E(config)# ethernet ring upstream-group <i>group-list</i>	<p>(Optional) configure RRPS uplink interface group.</p> <p> Note</p> <p>The uplink interface group must be used with failover. It supports dual homing topology. The uplink interface group corresponds to the failover group in one-to-one relationship.</p>

 **Note**

Master node election: at the beginning, all nodes consider themselves the master node, one of two interfaces is Block, so no data loop on the ring; when two interfaces on the ring node receive the same Hello packets for many times, the node considers that the ring topology is stable and can elect master node. Other nodes will not enable the blocked interface, usually only one master node, which ensures only one blocked interface, and ensures the connectivity of the nodes on the ring.

7.7.6 Checking configuration

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show ethernet ring [<i>ring-id</i>]	Show RRPS information.
2	Alpha-A28E# show ethernet ring port	Show RRPS interface information.
3	Alpha-A28E# show ethernet ring port statistic	Show statistics of RRPS interface packets.

7.7.7 Maintenance

Command	Description
Alpha-A28E(config)# clear ethernet ring <i>ring-id</i> statistics	Clear RRPS interface statistics, including RRPS ID, ring interface ID, Hello packet, Change packet, and Flush packet.

7.7.8 Example for configuring Ethernet ring

Networking requirements

As shown below, to improve the reliability of Ethernet, the Switch A, Switch B, Switch C, Switch D have constituted an Ethernet single ring Ring 1.

The figure shows that the four switches are added to Ring 1 interface. MAC addresses are Switch A (000E.5E00.000A), Switch B (000E.5E00.000B), Switch C (000E.5E00.000C), and Switch D (000E.5E00.000D).

The status and priority of four nodes are the same, MAC address of Switch D is biggest, and therefore, Switch D is the master node of RRPS.

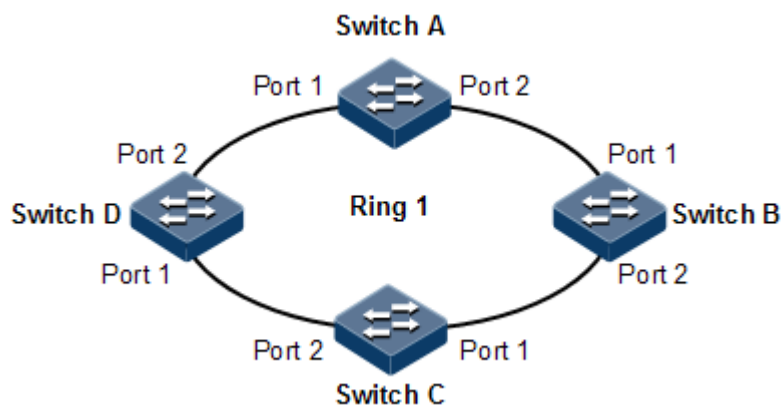


Figure 7-17 RRPS application networking

Configuration steps

Step 1 Configure Switch A.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#interface port 1
SwitchA(config-port)#ethernet ring 1 port 2
SwitchA(config-port)#exit
SwitchA(config)#ethernet ring 1 enable
```

Step 2 Configure Switch B, Switch C, and Switch D. Their configurations are the same as configurations of Switch A.

Checking result

Check RRPS configuration by the command of **show ethernet ring**.

Take Switch D for example, when the loop is normal, the first ring interface of master node Switch D: Port 1 block clears data loop.

```
SwitchD#show ethernet ring
Ethernet Ring Upstream-Group:--
Ethernet Ring 1:
Ring Admin:      Enable
Ring State:      Enclosed
Bridge State:    Block
Ring state duration: 0 days, 3 hours, 30 minutes, 15 seconds
Bridge Priority:  1
Bridge MAC:      000E.5E00.000D
Ring DB State:   Block
Ring DB Priority: 1
Ring DB:         000E.5E00.000D
Hello Time:      1
Restore delay:   5
Hold Time:       15
Protocol Vlan:   2
```

Break link simulation fault between Switch A and Switch B manually, Port 1 of Switch D will change its status from Block to Forwarding, Port 1 of Switch B will change its status from Forwarding to Block. Check RRPS status again.

```
SwitchD#show ethernet ring
Ethernet Ring Upstream-Group:1
Ethernet Ring 1:
Ring Admin:      Enable
Ring State:      Unenclosed
Bridge State:    Two-Forward
Ring state duration: 0 days, 3 hours, 30 minutes, 15 seconds
```



```
Bridge Priority: 1
Bridge MAC: 000E.5E00.000D
Ring DB State: Forwarding
Ring DB Priority: 1
Ring DB: 000E.5E00.000D
Hello Time: 1
Restore delay: 15
Hold Time: 15
Protocol Vlan: 2
```

8 OAM

This chapter describes basic principles and configuration procedures of OAM, including the following chapters:

- EFM
- CFM
- SLA

8.1 EFM

8.1.1 Introduction

Initially, Ethernet is designed for LAN. Operation, Administration and Maintenance (OAM) is weak for its small size and a NE-level administrative system. With continuous development of Ethernet technology, the application scale of Ethernet in telecom network becomes wider and wider. Compared with LAN, the link length and network size for telecom network is bigger and bigger. The lack of effective management and maintenance mechanism has seriously obstructed Ethernet technology applying to the telecom network.

To confirm connectivity of Ethernet virtual connection, effectively detect, confirm and locate faults on Ethernet layer, balance network utilization, measure network performance, and provide service according Service Level Agreement (SLA), implementing OAM on Ethernet has becoming an inevitable developing trend.

Ethernet OAM is realized in different levels, as show in Figure 8-1, and there are two levels:

- Link-level Ethernet OAM: it is applied in Ethernet physical link (that is the first mile) between Provider Edge (PE) and Customer Edge (CE), which is used to monitor link state between user network and operator network, and the typical protocol is Ethernet in the First Mile (EFM) OAM protocol.
- Business-level Ethernet OAM: it is applied in access aggregation layer of network, which is used to monitor connectivity of the whole network, locate connectivity fault of network, monitor and control performance of link, and the typical protocol is Connectivity Fault Management (CFM) OAM protocol.

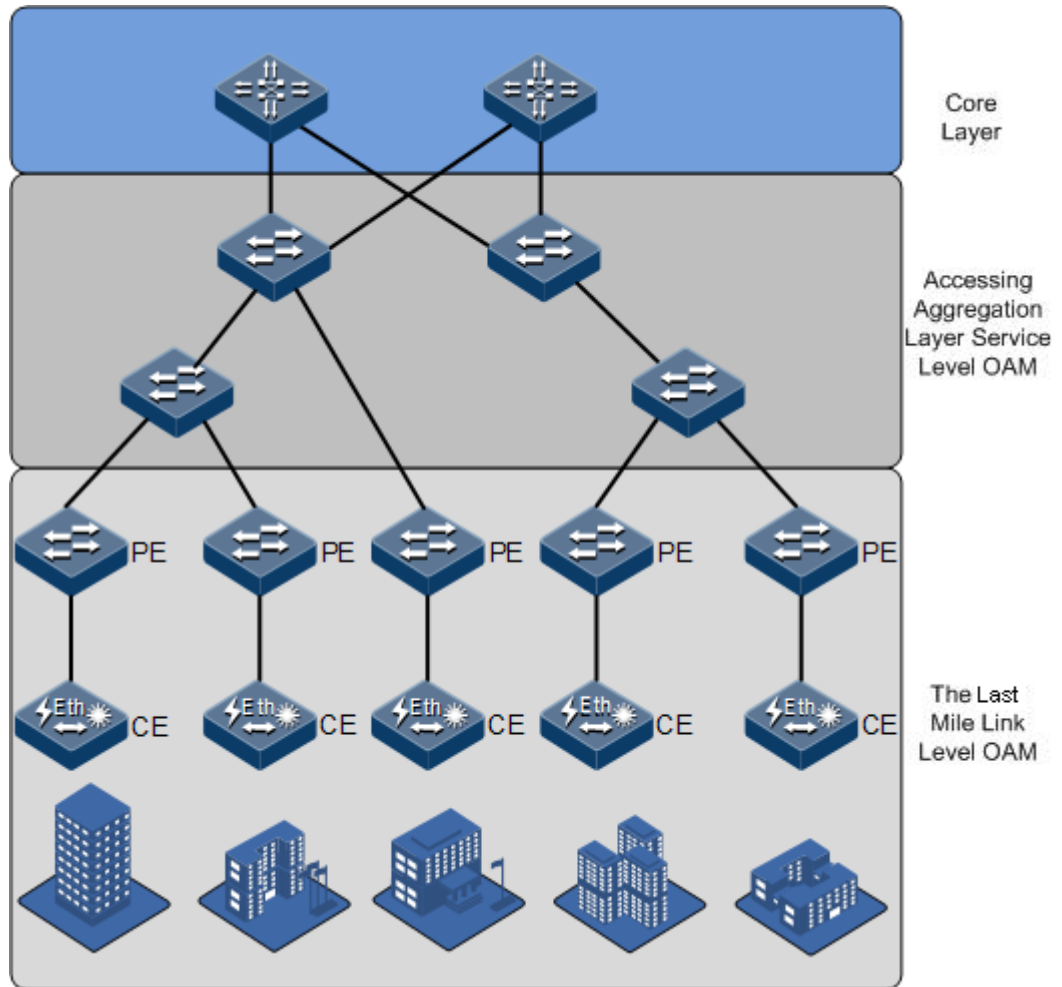


Figure 8-1 OAM classification

Complied with IEEE 802.3ah protocol, Ethernet in the First Mile (EFM) is a link-level Ethernet OAM technology. It provides the link connectivity detection, link fault monitor, and remote fault notification, etc. for a link between two directly connected devices.

"The first mile" in EFM is the connection between local device of telecom operator and client device. The target is that Ethernet technology will be extended to access network market of telecom users, in order to improve network performance, and reduce cost of device and running. EFM is mainly used in Ethernet link of user access network edge.

The A10E/A28E provides EFM with IEEE 802.3ah standard.

8.1.2 Preparing for configurations

Scenario

Deploying EFM between directly connected devices can effectively improve the management and maintenance capability of Ethernet links and ensure network running smoothly.

Prerequisite

Before configuring EFM, you need to connect interfaces and configure physical parameters on interfaces. Make the physical layer **Up**.

8.1.3 Default configurations of EFM

The default configuration of EFM is as below.

Function	Default value
EFM working mode	Passive mode
Sending interval of messages	10 × 100ms
Timeout of links	5s
OAM	Disable
Remote OAM event alarm function	Disable
EFM remote loopback state	Not response
Monitor window of error frame event	1s
Monitor threshold of error event	1 error frame
Monitor window of error frame period event	1000ms
Monitor threshold of error frame period event	1 error frame
Monitor window of link error frame second statistics event	60s
Monitor threshold of link error frame second statistics event	1s
Monitor window of link error coding statistics event	100ms
Monitor threshold of error coding statistic event	1s
Fault indication	Enable
Local OAM event alarm	Disable

8.1.4 Configuring basic functions of EFM

Configure basic functions of EFM for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)#oam { active passive }	Configure work mode for EFM. <ul style="list-style-type: none"> • Active: the device actively initiates OAM peer discovery process. In addition, the device supports responding to remote loopback command and variable obtaining request. • Passive: the device does not initiate OAM peer discovery process. In addition the device does not support sending remote loopback command and variable obtaining request.
3	Alpha-A28E(config)#oam send-period <i>period-number</i>	(Optional) OAM link connection is created by sending INFO message. Use this command to set interval of sending messages and control communication period of link. The unit is 100ms.
4	Alpha-A28E(config)#oam timeout <i>period-number</i>	(Optional) Set OAM link timeout. When both ends of OAM link do not receive OAM message in the interval and the interval is longer than the timeout, the OAM link breaks down. The unit is second.
5	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
6	Alpha-A28E(config- port)# oam enable	Enable EFM OAM on an interface.

8.1.5 Configuring active functions of EFM

Configure active functions of EFM for the A10E/A28E as below.



Note

The active EFM must be configured when the A10E/A28E is in active mode.

(Optional) configuring the A10E/ A28E initiating EFM remote loopback

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical interface configuration mode.
3	Alpha-A28E(config- port)# oam remote- loopback	Configure initiating EFM remote loopback on an interface. The remote loopback can be initiated only when EFM is connected and configured working in active mode.

Step	Configuration	Description
4	Alpha-A28E(config-port)#no oam remote-loopback	(Optional) disable remote loopback. After detection, disable remote loopback immediately.



Note

You can discover network faults in time by periodically detecting loopbacks. By detecting loopbacks in segments, you can locate exact areas where faults occur and you can troubleshoot these faults.

When a link is in loopback status, the A10E/A28E detects all packets but OAM packets received by the link. Therefore, disable this function immediately when no detection is needed.

(Optional) configuring peer OAM event alarm

Step	Configuration	Description
1	Alpha-A28E#config	Enter global configuration mode.
2	Alpha-A28E(config)#interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)#oam peer event trap enable	Enable peer OAM event trap and then link monitoring event can be reported to NMS center in time. By default, device does not report trap to NMS center through SNMP TRAP when receiving peer link monitoring event.

(Optional) viewing current variable information about the peer device

Step	Configuration	Description
1	Alpha-A28E#show oam peer [link-statistic oam-info] [port-list port-list]	Get OAM information or variable values about the peer device.



Note

By getting the current variable of the peer, you can get status of current link. IEEE802.3 Clause 30 defines and explains supported variable and its denotation gotten by OAM in details. The variable takes Object as the maximum unit. Each object contains Package and Attribute. A package contains several attributes. Attribute is the minimum unit of a variable. When getting an OAM variable, it defines object, package, branch and leaf description of attributes by Clause 30 to describe requesting object, and the branch and leaf are followed by variable to denote object responds variable request. The A10E/A28E supports getting OAM information and interface statistics.

Peer variable cannot be gotten until EFM is connected.

8.1.6 Configuring passive functions of EFM

Configure passive functions of EFM for the A10E/A28E as below.



Note

The passive EFM can be configured regardless the A10E/A28E is in active or passive mode.

(Optional) configuring the A10E/ A28E responding to EFM remote loopback

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# oam loopback { ignore process }	Configure the A10E/A28E responding to/ignoring EFM remote loopback. By default, the A10E/A28E responds to OAM remote loopback.



Note

The peer EFM remote loopback will not take effect until the remote loopback response is configured on the local device.

(Optional) configuring OAM link monitoring

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# oam errored-frame window window threshold threshold	Configure the monitor window and threshold for an error frame event.
4	Alpha-A28E(config-port)# oam errored-frame-period window window threshold threshold	Configure the monitor window and threshold for an error frame period event.
5	Alpha-A28E(config-port)# oam errored-frame-seconds window window threshold threshold	Configure the monitor window and threshold for an error frame seconds event.
6	Alpha-A28E(config-port)# oam errored-symbol-period window window threshold threshold	Configure the monitor window and threshold for an error symbol period event.



Note

The OAM link monitoring is used to detect and report link errors in different conditions. When detecting a fault on a link, the A10E/A28E provides the peer with the generated time, window and threshold setting, etc. by OAM event notification packets. The peer receives event notification and reports it to the NMS center via SNMP Trap. Besides, the local device can directly report events to the NMS center via SNMP Trap. By default, the system sets default value for error generated time, window and threshold setting.

(Optional) configuring OAM fault indication

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# oam notify { critical-event dying-gasp errored-frame errored-frame-period errored-frame-seconds errored-symbol-period } { disable enable }	Configure OAM fault indication, which is used to inform the peer when the local fails. Faults that can be notified to the peer contain link-fault, dying-gasp, and critical-event. By default, OAM fault indication is enabled. When a fault occurs, the local device notifies the peer through OAM. The link-fault fault must be notified to the peer while the dying-gasp and critical-event faults can be disabled by this command.

(Optional) configuring local OAM event alarm

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# oam event trap enable	Enable local OAM event alarm and then link monitoring event can be reported to NMS center in time.

8.1.7 Checking configurations

Use the following commands to check configuration results.

Step	Configuration	Description
1	Alpha-A28E# show oam [port-list <i>port-list</i>]	Show EFM basic information.

Step	Configuration	Description
2	Alpha-A28E# show oam loopback [port-list <i>port-list</i>]	Show EFM remote loopback configurations.
3	Alpha-A28E# show oam notify [port-list <i>port-list</i>]	Show OAM link monitoring and fault indication configurations.
4	Alpha-A28E# show oam statistics [port-list <i>port-list</i>]	Show OAM statistics.
5	Alpha-A28E# show oam trap [port-list <i>port-list</i>]	Show OAM event alarm configurations.
6	Alpha-A28E# show oam event [port-list <i>port-list</i>] [critical]	Show information about local critical faults detected on an interface.
7	Alpha-A28E# show oam peer event [port-list <i>port-list</i>] [critical]	Show information about critical faults sent by the peer.

8.1.8 Maintenance

You can maintain the EFM feature through the below command.

Command	Description
Alpha-A28E(config-port)# clear oam statistics	Clear EFM OAM interface link statistics.
Alpha-A28E(config-port)# clear oam event	Clear EFM OAM interface link event information.

8.1.9 Example for configuring EFM

Networking requirements

As shown in Figure 8-2, to improve the management and maintenance capability of the Ethernet link between Switch A and Switch B, you need to deploy EFM on Switch A. Switch A works in active mode and is deployed with OAM event alarm function.



Figure 8-2 Configuring EFM

Configuration steps

Step 1 Configure Switch A.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#oam active
SwitchA(config)#interface port 1
SwitchA(config-port)#oam enable
SwitchA(config-port)#oam event trap enable
SwitchA(config-port)#oam peer event trap enable
```

Step 2 Configure Switch B.

```
Alpha-A28E#hostname SwitchB
SwitchB#config
SwitchB(config)#interface port 1
SwitchB(config-port)#oam enable
```

Checking results

Show EFM configurations on Switch A by the command of **show oam**.

```
SwitchA#show oam port-list 1
Port: 1
Mode:Active
Administrate state: Enable
Operation state: Operational
Max OAMPDU size: 1518
Send period: 1000 ms
Link timeout : 5 s
Config revision: 1
Supported functions: Loopback, Event, Variable
```

Show OAM event alarm configurations on Switch A by the command of **show oam trap**.

```
SwitchA#show oam trap port-list 1
Port: 1
Event trap: Enable
Peer event trap: Enable
Discovery trap total: 0
Discovery trap timestamp: 0 days, 0 hours, 0 minutes
Lost trap total: 0
Lost trap timestamp: 0 days, 0 hours, 0 minutes
```

8.2 CFM

8.2.1 Introduction

Connectivity Fault Management (CFM) is end to end service level Ethernet OAM technology, implementing end-to-end connectivity fault detection, fault notification, judgement and location functions. This function is used to actively diagnose fault for Ethernet Virtual Connection (EVC) and provide cost-effective network maintenance solution via fault management function and improve network maintenance.

The Device provides CFM function that compatible ITU-Y.1731 and IEEE802.1ag recommendations.

CFM Component

CFM is made from below components:

- MD

Maintenance Domain (MD, also called MEG, Maintenance Entity Group) is a network that runs CFM function. It defines network range for OAM management. MD has level property with 8 different levels (level 0 to level 7), the greater the number is, the higher the level is, and the larger the range is. Protocol packets of a lower level MD will be discarded when entering a higher level MD; while the higher level MD packets can transmit through the lower level MD. In one VLAN range, different MDs can be adjacent, embedded, crossed over.

As shown in Figure 8-3, MD2 is contained in MD1. MD1 packets need to transmit through MD2. Configure MD1 level as 6, and MD2 level as 3. Then MD1 packets can traverse through MD2 and implement connectivity fault management of whole MD1, but MD2 packets will not diffuse into MD1. MD2 is server layer and MD1 is client layer.

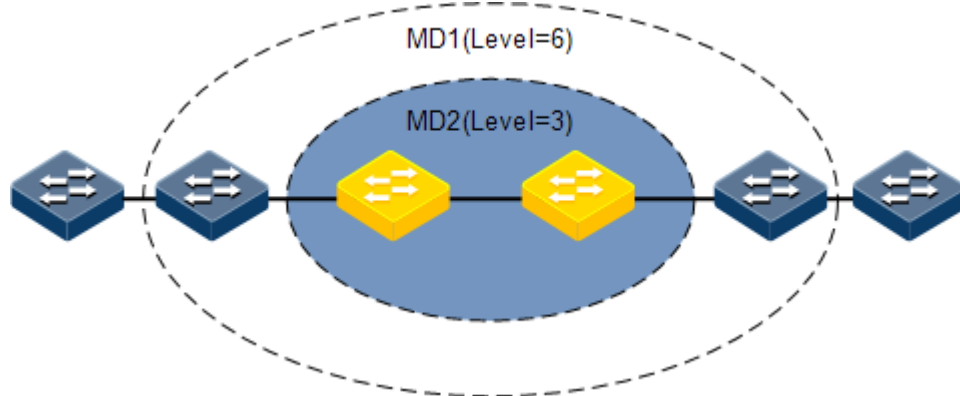


Figure 8-3 Different MD Levels

- Service instance

Service Instance also called Maintenance Association (MA) is part of MD. One MD can be divided into one or multiple service instances. One service instance corresponds to one service, mapping to one VLAN group, VLAN of different service instances cannot crossover. Though service instance can mapping to multiple VLAN, one instance can use one VLAN for transmitting or receiving OAM packets. The VLAN is master VLAN of the instance.

- MEP

As shown in Figure 8-4, Maintenance associations End Point (MEP) is edge node of service instance. MEP can transmit and deal with CFM packets, instance that MEP located and MD decide MEP transmit and receive packets VLAN and level.

MEP on any device set running CFM in network is called local MEP; MEP on other devices in this instance is called Remote Maintenance association End Point (RMEP).

One instance can configure multiple MEP, packets sent by MEP in one instance take identical S-VLAN TAG and with identical priority and C-VLAN TAG. MEP can receive OAM packets sent by other MEP in the instance and stop packets with the same level or lower than itself.

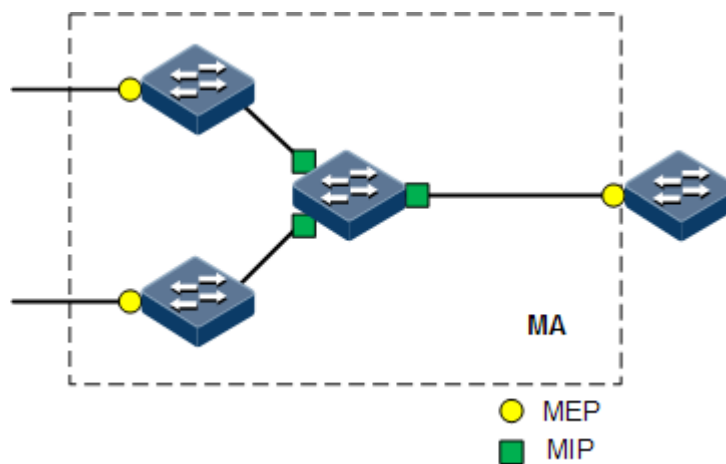


Figure 8-4 Network Sketch Map of MEP and MIP

- MIP

As shown in Figure 8-4, Maintenance association Intermediate Point (MIP) is inner node of service instance, automatically created by the A10E/A28E. MIP cannot send CFM packets actively but can process and answer LinkTrace Message (LTM) and LoopBack Message (LBM) packets.

- MP

MEP and MIP are Maintenance Points (MPs).

8.2.2 Preparing for configurations

Scenario

To develop Ethernet technology application in telecommunication network, Ethernet needs to realize service level identical to telecommunication transmission network. CFM provides full OAM tool to solve this problem through telecommunication Ethernet.

CFM provides the below OAM functions:

- Fault detection function (CC, Continuity Check)
This function is realized by MEP sends Continuity Check Packet (CCM) periodically, other MEP in one service instance receives packet to confirm status of RMEP. If the A10E/A28E faulty or link configuration is incorrect, MEP cannot receive and process CCM from RMEP. If MEP has not received remote CCM packet in 3.5 CCM intervals, the link is considered to be fault, system will send fault trap according to alarm priority configuration.
- Fault acknowledgement function (LB, LoopBack)
This function confirms connectivity between two MP by sending LBM from source MEP and answering LoopBack Reply (LBR) by destination MP. Source MEP sends LBM to MP for fault acknowledgement, the MP receives LBR and sends a LBR to source MEP,

if source MEP received LBR the path is connective, if source MEP does not receive LBR the path is not connective.

- Fault location function (LT, LinkTrace)
Source MEP sends LTM (LinkTrace Packet) to destination MP, each MP device on LTM transmitting path answers LTR (LinkTrace Reply) to source MEP, the function records efficient LTR and LTM fault location point.

Anyway, CFM implements end-to-end service OAM technology, reducing carriers' operation cost and improving competitiveness.

Prerequisite

- Connect the interface and configure physical parameters for it to make it physically Up.
- Create VLANs.
- Add interfaces into VLANs.

8.2.3 Default configurations of CFM

Function	Default value
Global CFM function status	Disable
CFM function status on interface	Enable
MEP status based on service instance	Up direction
Aging time of RMEP	100min
Storage time of error CCM packet	100min
MEP sending CCM packet status	Not send
MEP sending CCM packet mode	Passive mode
CCM packet sending interval	1s
Dynamic import function of service instance RMEP learning	Not take effect
cc check function of RMEP	Disable
Priority of CFM OAM packet	6
Layer-2 ping function status	The number of sending LBM packets is 5; the length of packet TLV is 64.
Switch status of fault location data base	Disable
Storage time of fault location data base	100min
Alarm suppression function status	Enable

8.2.4 Enabling CFM

Configure CFM for the A10E/A28E as below.





CFM fault detection, location function cannot take effect unless enables CFM function on the A10E/A28E.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ethernet cfm enable	Enable global CFM function.
3	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
4	Alpha-A28E(config-port)# ethernet cfm enable	Enable CFM on interface. Use the ethernet cfm disable command to disable this function. After it is disabled, the interface cannot receive or send CFM packets.

8.2.5 Configuring basic CFM functions

Configure CFM for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ethernet cfm domain [md-name domain-name] level level	Create maintain domain. Use the parameter md-name to assign name for MD in 802.1ag style. MA and CCM packets under MD are both in 802.1ag style; do not assign name, the MD is in Y.1731 style, MA and CCM packets under this MD are both in Y.1731 style. If user assigns name for MD, the name must be unique in global, or else MD configuration will be failure.  Note Level of different MD must be different; otherwise MD configuration will fail.
3	Alpha-A28E(config)# service cisid level level	Create service instance and enter instance configuration mode (MD name, service instance name). Character string is unique in global range. If service instance existed, this command will direct lead to service instance configuration mode.


Step	Configuration	Description
4	Alpha-A28E(config-service)# service vlan-list <i>vlan-list</i>	<p>Configure service application VLAN map.</p> <p>VLAN list permits at most 32 VLAN. The smallest VLAN will be taken as primary VLAN of service instance. All MEP in service instance transmit and receive packets through primary VLAN.</p> <p> Note</p> <p>Since using primary VLAN to transmit and receive packets, all of other VLAN in the list are mapped to primary VLAN. This logical VLAN mapping relationship is globally; VLAN mapping relationship of different level can be identical but cannot crossover. For example: instance 1 mapping to VLAN 10-20, instance 2 mapping to VLANs 15-30, the configuration is illegal because VLANs 15-20 are crossed.</p>
5	Alpha-A28E(config-service)# service mep [up down] mpid <i>mep-id</i> port <i>port-id</i>	<p>Configure MEP over service instance.</p> <p>Service instance must map to VLAN when configuring this kind MEP. By default, MEP is Up direction, namely interface uplink direction detects fault.</p>

8.2.6 Configuring fault detection

Configure CFM fault detection on the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# ethernet cfm remote mep age-time <i>minute</i>	(Optional) configure RMEP aging time.
3	Alpha-A28E(config)# ethernet cfm errors archive-hold-time <i>minute</i>	<p>(Optional) configure hold time for error CCM packets. The A10E/A28E saves all fault information of reported by MEP.</p> <p>By default, hold time for error CCM packets is 100 minutes. It check data in database once system configures new hold time, clear data immediately if there is data over time.</p>
4	Alpha-A28E(config)# ethernet cfm mode { slave master }	Configure the mode for all service instances to send CCM packets.
5	Alpha-A28E(config)# service cisid level <i>level</i>	Enter service instance configuration mode.

Step	Configuration	Description
6	Alpha-A28E(config-service)# service cc interval { 1 10 100ms 60 600 }	(Optional) configure service instance CCM packets sending time interval. By default, CCM packets sending time interval is 10 seconds. Cannot modify CCM packets sending interval when CCM packets sending function enable.
7	Alpha-A28E(config-service)# service cc enable mep { <i>mep-list</i> all }	Enable MEP sending CCM packets. By default, MEP does not send CCM packet.
8	Alpha-A28E(config-service)# service remote-mep <i>mep-list</i>	(Optional) configure static RMEP. Used cooperated with cc check function.
9	Alpha-A28E(config-service)# service remote-mep learning active	(Optional) configure RMEP learning dynamic import function. Service instance transfer dynamic RMEP to static RMEP by automation every time receiving of CCM packets. By default, this function does not take effective.
10	Alpha-A28E(config-service)# service remote-mep cc-check enable	(Optional) configure RMEP cc check function. After this function is enabled, system checks dynamic learned RMEP ID consistent with static RMEP ID when receiving CCM packets, if not consistent, the CCM packets are considered as incorrect.
11	Alpha-A28E(config-service)# service cvlan <i>vlan-id</i>	(Optional) configure client VLAN of CFM OAM packets, just need configure in QinQ networking environment. By default, CFM OAM packets do not take C-TAG. After configuring client VLAN for service instance, all MEP under the instance send CCM, LTM, LBM, DMM with double TAG. Hereinto, C-TAG uses this command to configure client VLAN.
12	Alpha-A28E(config-service)# service priority <i>priority</i>	(Optional) configure CFM OAM packets priority. After configuring packets priority, all CCM, LBM, LTM, DMM sent by MEP use assigned priority.

Step	Configuration	Description
	<pre>Alpha-A28E(config- service)#snmp-server trap cfm { all ccmerr macremerr none remerr xcon } mep { all mep-list }</pre>	<p>(Optional) configure CFM permits sending fault trap type.</p> <p>CC function of CFM can detect fault in 5 levels, the order from high to low: level 5–cross connection, level 4-CCM error, level 3-loss of RMEP, level 2-interface status fault, level 1-RDI. By default, it is macremerr, namely permit fault trap on level 2-5.</p> <p> Note</p> <ul style="list-style-type: none"> • When CFM detected fault, identical level or lower level fault will not generate trap again before removing fault; • Wait for 10s until the fault status is cleared after removing CFM fault.

8.2.7 Configuring fault acknowledgement

Configure CFM fault acknowledgement for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# service cisid level level	Enter service instance configuration mode.
3	Alpha-A28E(config-service)# ping { <i>mac-address</i> mep rmep-id } [count count] [size size] [source mep-id]	<p>Execute Layer 2 ping function for acknowledging fault.</p> <p>By default, sending LBM packets number is 5, packets TLV size is 64, search an available source MEP by automation.</p> <p>CFM needs to find destination MEP MAC address to execute ping operation if perform Layer 2 ping operation by assigning destination MEPID. After source MEP discovers RMEP and becomes stable, it saves data information of RMEP in RMEP database, and then RMEP MAC address can be found from RMEP database according to MEPID.</p>

 **Note**

- Make sure global CFM function enable before executing this command, otherwise the command will be executed unsuccessfully;
- If there is no MEP configured in service instance, ping unsuccessfully because of fail to find source MEP;

- If assigned source MEP is invalid, ping unsuccessfully. For example, assigned source MEP is not existing or CFM of the source MEP interface is disabled;
- If assigning destination MEP ID to perform ping operation, ping unsuccessfully when fail to find destination MEP MAC address according to MEPID;
- Operation unsuccessful if other users are using the assigned source MEP to perform ping operation.

8.2.8 Configuring fault location

Configure CFM fault location for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# confi g	Enter global configuration mode.
2	Alpha-A28E(config)# ethe rnet cfm traceroute cache enable	(Optional) enable fault location database function. In enable status, system trace route information via database storing protocol, the command of show ethernet cfm traceroute cache can show at any time. In disable status, result of traceroute will be cleared after executing traceroute. Disable by default, the command of ethernet cfm traceroute cache disable can disable it.
3	Alpha-A28E(config)# ethe rnet cfm traceroute cache hold-time <i>minute</i>	(Optional) configure data hold time for fault location database. You can set data hold time when fault location database function is enabled. Hold time is 100 minutes by default.
4	Alpha-A28E(config)# ethe rnet cfm traceroute cache size <i>size</i>	(Optional) configure saved data amount. You can set the saved data amount when the function is enabled. It is 100 by default; does not save data if the function is disabled.
5	Alpha-A28E(config)# serv ice cisid level <i>level</i>	Enter service instance configuration mode.
6	Alpha-A28E(config- service)# tracero ute { mac-address mep mep-id } [ttl ttl] [source mep-id]	Execute Layer 2 Traceroute function for fault locating. By default, packets TLV size is 64, search an available source MEP by automation. CFM should find MAC address of destination MEP by mep-id to complete traceroute operation if Layer 2 traceroute operation is operated by specified destination mep-id. Users can find the following content by data base of RMEP: data information of RMEP is saved in RMEP database in MEP after source MEP found RMEP and it is stable, you can find MAC address of RMEP according to mep-id in RMEP database.



Note

- Make sure global CFM function enable before executing this command, otherwise the command will be executed unsuccessfully;

- If there is no MEP configured in service instance, Traceroute unsuccessfully because of fail to find source MEP;
- If assigned source MEP is invalid, Traceroute unsuccessfully. For example, assigned source MEP is not existing or CFM of the source MEP interface is disabled;
- If assigning destination MEPID to perform Traceroute operation, Traceroute unsuccessfully when fail to find destination MEP MAC address according to MEPID;
- If CC function is not effective, configure static RMEP and assign MAC address to ensure Layer 2 traceroute operating successfully;
- Operation unsuccessful if other users are using the assigned source MEP to perform Traceroute operation.

8.2.9 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show ethernet cfm	Show CFM global configuration.
2	Alpha-A28E# show ethernet cfm domain [level level]	Show MD and service instance configuration.
3	Alpha-A28E# show ethernet cfm errors [level level]	Show error CCM database information.
4	Alpha-A28E# show ethernet cfm local-mp [interface port port-id level level]	Show Ethernet locked signals.
5	Alpha-A28E# show ethernet cfm remote-mep [static]	Show local MEP configuration.
7	Alpha-A28E# show ethernet cfm remote-mep [level level [service name [mpid local-mep-id]]]	Show static RMEP information.
8	Alpha-A28E# show ethernet cfm traceroute-cache	Show RMEP discovery information.
9	Alpha-A28E# show ethernet cfm traceroute-cache	Show database trace route information.

8.2.10 Maintenance

Maintain the A10E/A28E as below.

Command	Description
Alpha-A28E(config)# clear ethernet cfm errors [level level]	Clear CCM error database information.
Alpha-A28E(config)# clear ethernet cfm remote-mep [level level]	Clear RMEP.
Alpha-A28E(config)# clear ethernet cfm traceroute-cache	Clear traceroute cache database.

8.2.11 Example for configuring CFM

Networking requirements

As shown in Figure 8-5, the PC communicates with the server through the network consisting of by Switch A, Switch B and Switch C. You can deploy CFM feature on Switch Device to realize active fault detection, acknowledgement and location, then make Ethernet link between PC and Server achieving telecommunication service level. Switch A and Switch C are MEP, Switch B is MIP, detecting Ethernet fault from Switch A Port 1 to Switch C Port 2, maintenance domain level is 3.

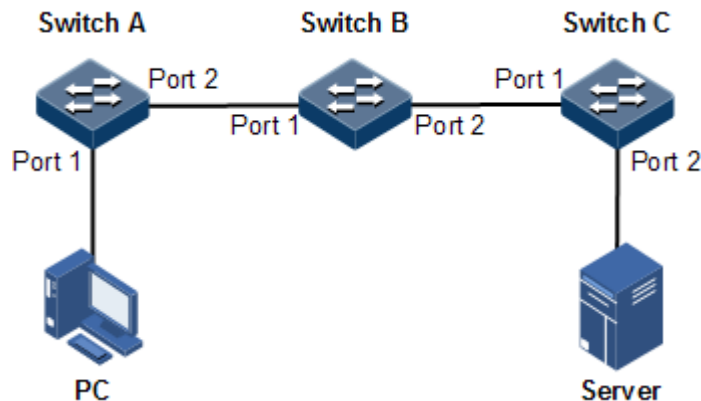


Figure 8-5 CFM application

Configuration steps

Step 1 Configure interface adding into VLAN.

Configure Switch A.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100 active
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport access vlan 100
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
```

Configure Switch B.

```
Alpha-A28E#hostname SwitchB
SwitchB#config
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
```

```
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
```

Configure Switch C.

```
Alpha-A28E#hostname SwitchC
SwitchC#config
SwitchC(config)#create vlan 100 active
SwitchC(config)#interface port 2
SwitchC(config-port)#switch access vlan 100
SwitchC(config-port)#exit
SwitchC(config)#interface port 1
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
```

Step 2 Configure CFM fault detection function.

Configure Switch A.

```
SwitchA(config)#ethernet cfm domain level 3
SwitchA(config)#service ma1 level 3
SwitchA(config-service)#service vlan-list 100
SwitchA(config-service)#service mep up mpid 301 port 1
SwitchA(config-service)#service remote-mep 302
SwitchA(config-service)#service cc enable mep all
SwitchA(config-service)#exit
SwitchA(config)#ethernet cfm enable
```

Configure Switch B.

```
SwitchB(config)#ethernet cfm domain level 3
SwitchB(config)#service ma1 level 3
SwitchB(config-service)#service vlan-list 100
SwitchB(config-service)#exit
SwitchB(config)#ethernet cfm enable
```

Configure Switch C.

```
SwitchC(config)#ethernet cfm domain level 3
SwitchC(config)#service ma1 level 3
SwitchC(config-service)#service vlan-list 100
SwitchC(config-service)#service mep up mpid 302 port 2
SwitchC(config-service)#service remote mep 301
SwitchC(config-service)#service cc enable mep all
SwitchC(config-service)#exit
```

```
SwitchC(config)#ethernet cfm enable
```

Step 3 Execute CFM fault acknowledgement.

Take Switch A as an example.

```
Switch(config)#service ma1 level 3  
Switch(config-service)#ping mep 302 source 301  
Sending 5 ethernet cfm loopback packets to 000e.5e03.688d, timeout is 2.5  
seconds:  
!!!!  
Success rate is 100 percent (5/5).  
Ping statistics from 000e.5e03.688d:  
Received loopback replys:< 5/0/0 > (Total/Out of order/Error)  
Ping successfully.
```

Step 4 Execute CFM fault location.

Take Switch A as an example.

```
SwitchA(config-service)#traceroute mep 302 source 301  
TTL: <64>  
Tracing the route to 000E.5E00.0002 on level 3, service ma1.  
Traceroute send via port1.  
-----  
Hops  HostMac          Ingress/EgressPort  IsForwarded  RelayAction  NextHop  
-----  
1     000E.5E00.0003    2/1                 Yes          rlyFdb      000E.5E00.0003  
2     000E.5E00.0003    1/2                 Yes          rlyFdb      000E.5E00.0001  
3     000E.5E00.0001    1/-                 No           rlyHit      000E.5E00.0002
```

Checking result

Show CFM configuration on Switch by the command of **show ethernet cfm**.

Take Switch A as an example.

```
SwitchA#show ethernet cfm  
Global cfm Status: enable  
Port CFM Enabled Portlist: 1-10  
Archive hold time of error CCMs: 100(Min)  
Remote mep aging time: 100(Min)  
Device mode: slave
```

8.3 SLA

8.3.1 Introduction

SLA is a telecommunication service evaluation standard negotiated by the service provider and users. It is an agreement in service quality, priority and responsibility, etc.

In technology, SLA is real-time network performance detection and statistic technique for responding time, network jitter, delay, packet loss rate, etc. SLA can choose different operations to monitor measurement values for different applications.

The

- Operation

It is a static concept. It is SLA network performance testing task from end to end, including delay/jitter test (y1731-jitter/y1731-pkt-loss) on the Layer 2 network and delay/jitter test (ICMP-echo/ICMP-jitter) on the Layer 3 network.

- Test

It is a dynamic concept. It is used to describe an execution of one operation.

- Detection

It is a dynamic concept. It is used to describe a procedure of transmitting-receiving packet in operation test. According to definition of operation, one operation test can contain multiple detections (a test only contains only one detection for Echo operation).

- Schedule

It is a dynamic concept. It describes a schedule of one operation. One schedule contains multiple periodical test execution.

8.3.2 Preparing for configurations

Scenario

The carrier and users sign SLA protocol to guarantee users can enjoy certain quality network service. To perform SLA protocol effectively, carrier needs to deploy SLA feature test performance on the A10E/A28E and the test result is evidence to ensure user's performance.

SLA feature chooses two testing node, configure SLA operation on one node and schedule executing it to implement network performance test between the two nodes.

SLA takes statistics of round-trip packet loss rate, round-trip or unidirectional (SD/DS) delay, jitter, jitter variance, jitter distribution, etc, and informs the upper monitoring software (such as NMS) of these data, analyse network performance, and provide data required by the user.

Prerequisite

- Deploy CFM between the tested devices.
- Configure IP (scheduling of icmp-echo and icmp-jitter).

8.3.3 Default configurations of SLA

Function	Default value
SLA scheduling status	Disable
SLA Layer 2 operation CoS	Level 0
SLA jitter operation detection interval	1s
Number of SLA jitter operation detection packets	10
Life period of SLA scheduling operation	forever
Test period of SLA scheduling operation	300s

8.3.4 Creating SLA operations

Configure the A10E/A28E as below.


Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# sla oper-num y1731-echo remote-mep mep-id level level svlan vlan-id [cvlan vlan-id] [cos cos-value]	Configure SLA y1731-jitter operation according to the destination MEP ID.
3	Alpha-A28E(config)# sla oper-num y1731-jitter remote-mep mep-id level level svlan vlan-id [cvlan vlan-id] [cos cos-value] [interval period] [packets packets-num]	Configure SLA y1731-jitter operation according to the destination MEP.
4	Alpha-A28E(config)# sla oper-num icmp-echo dest-ipaddr ip-address [dscp dscp-value]	Configure basic information about SLA icmp-echo operation.
5	Alpha-A28E(config)# sla oper-num icmp-jitter dest-ipaddr ip-address [dscp dscp-value] [interval period] [packets packets-num]	Configure basic information about SLA icmp-jitter operation.
6	Alpha-A28E(config)# sla y1731-echo quick-input [level level] [svlan vlan-id]	Quickly create an y1731-echo operation.
7	Alpha-A28E(config)# sla y1731-jitter quick-input [level level] [svlan vlan-id]	Quickly create an y1731-jitter operation.



- After basic information of an operation (distinguished by operation number) is configured, the operation cannot be modified or reconfigured. If you need to modify the operation, delete the operation and then reconfigure it.
- SLA supports at most 100 operations being scheduled at one time, but wait a schedule to finish (reach schedule life time or stop schedule) before schedule again or modify schedule information.

8.3.5 Configuring SLA scheduling

Configure SLA scheduling information for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# sla schedule <i>oper-num</i> [life { forever <i>life-time</i> }] [period <i>period</i>] [begin]	Configure SLA operation scheduling information, and enable SLA operation scheduling. By default, SLA operation scheduling is disabled.  If you use the begin parameter, the configuration will be loaded upon device startup, without actual scheduling operations. If you does use the begin parameter, scheduling operations will be performed.

8.3.6 Checking configuration

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show sla { all <i>oper-num</i> } configuration	Show SLA configurations.
2	Alpha-A28E# show sla { all <i>oper-num</i> } result	Show test information of last SLA operation.
3	Alpha-A28E# show sla { all <i>oper-num</i> } statistic	Show statistics of operation scheduling. The same operation (distinguished by operation number) can be taken statistics of for 5 groups. If more groups have to be taken statistics of, the oldest (according to start time of scheduling) group will be aged.

8.3.7 Example for configuring SLA

Networking requirements

As shown in Figure 8-6, the PC communicates with the server through the network consisting of by Switch A, Switch B and Switch C. You can deploy CFM feature on switches to make the Ethernet link between the server and the PC to reach the telecom-grade level. SLA is deployed on Switch A to effectively carry out SLA agreement signed with the users. SLA is periodically scheduled to test the network performance between Switch A and Switch C.

Conduct Layer 2 delay test on Switch A towards Switch C. Configure the y1731-echo operation on Switch A, with operation number of 2, remote MEP of 2, MD level of 3, VLAN ID of 100, CoS of 0, life period of scheduling of 20s, and test period of 10s.

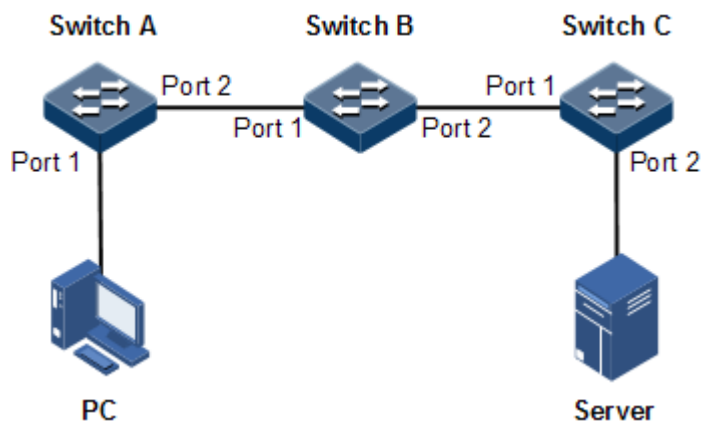


Figure 8-6 SLA application networking

Configuration steps

Step 1 Configure CFM on Switches.

For details, see section 8.2.11 Example for configuring CFM.

Step 2 Configure y1731-echo operation on Switch A, and enable operation scheduling.

```
SwitchA#config
SwitchA(config)#sla 2 y1731-echo remote-mep 302 level 3 svlan 100 cos 0
SwitchA(config)#sla schedule 2 life 20 period 10
```

Checking configurations

Use the **show sla configuration** command on Switch B to see whether SLA configurations are correct.

```
Switch_B#show sla 1 configuration
```

```
-----
operation <1>:
```

```
Type: y1731-JITTER
Frame Type: Delay Measurement
```

```
Cos: 0
Service Vlan ID: 3
MD Level: 3
Remote DEST MAC: 000E.5E00.0001
Timeout(sec): 1
Jitter Interval(msec): 1000
Measurement interval(sec): 10
Schedule Life(sec): 20
Schedule Status: No Active
```

Use the **show sla configuration** command on Switch C to see whether SLA configurations are correct.

Alpha-A28E#show sla 2 configuration

```
Operation <2>:
Type: Y.1731 echo
pkt Type: 1b
Starttime: 0 days, 0:0:0
```

```
Cos: 0
Service Vlan ID: 100
Customer Vlan ID: 0
MD Level: 3
Remote MEP ID: 302
Timeout(sec): 5
Schedule Life(sec): 20
Schedule Period(sec): 10
Schedule Status: Completed!
```

9 System management

This chapter introduces basic principle and configuration of system management and maintenance, and provides related configuration applications.

- SNMP
- KeepAlive
- RMON
- **Ошибка! Источник ссылки не найден.**
- LLDP
- Extended OAM
- Optical module DDM
- System log
- Power monitoring
- CPU monitoring
- Ping
- Traceroute

9.1 SNMP

9.1.1 Introduction

Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to resolve problems in managing network devices connected to the Internet. Through SNMP, a network management system can manage all network devices that support SNMP, including monitoring network status, modifying configurations of a network device, and receiving network alarms. SNMP is the most widely used network management protocol in TCP/IP networks.

Working mechanism

SNMP is separated into two parts: Agent and NMS. The Agent and NMS communicate by SNMP packets being sent through UDP. The working system of SNMP is shown in Figure 9-1.

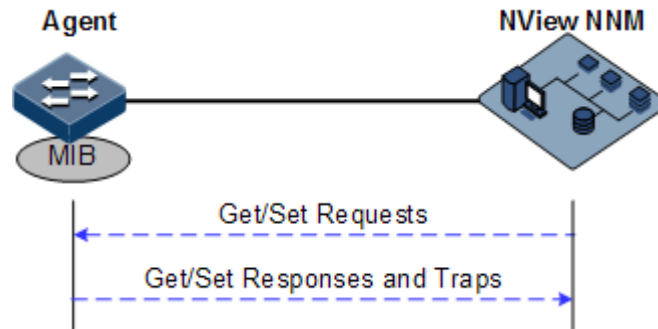


Figure 9-1 Working mechanism of SNMP

Orion NView NNM system can provide friendly Human Machine Interface (HMI) to facilitate network management. The below functions can be realized through it:

- Send request packets to the managed device.
- Receive reply packets and Trap packets from the managed device, and show result.

Agent is a program stays in the managed device, realizing the below functions:

- Receive/reply request packets from NView NNM system
- Read/write packets and generate response packets according to the packets type, then return the result to NView NNM system
- Define trigger condition according to protocol modules, enter/exit from system or reboot device when conditions are satisfied; reply module sends Trap packets to NView NNM system via agent to report current status of device.



Note

Agent can be configured with several versions. Agent use different versions to communicate with different Nview NNM systems. However, SNMP version of the NView NNM system must be consistent with the one on Agent when they are communicating. Otherwise, they cannot communicate properly.

Protocol versions

Till now, SNMP has three versions: v1, v2c, and v3, described as below.

- SNMP v1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a secret. The network management system can visit the agent only by specifying its community name correctly. If the community name carried in a SNMP message is not accepted by the A10E/A28E, the message will be dropped.
- Compatible with SNMP v1, SNMP v2c also uses community name authentication mechanism. SNMP V2c supports more operation types, data types, and error codes, and thus better identifying errors.
- SNMP v3 uses User-based Security Model (USM) and View-based Access Control Model (VACM) security mechanism. You can configure whether USM authentication is enabled and whether encryption is enabled to provide higher security. USM authentication mechanism allows authenticated senders and prevents unauthenticated senders. Encryption is to encrypt messages transmitted between the network management system and agents, thus preventing interception.

The A10E/A28E supports v1, v2c, v3 of SNMP.

MIB

Management Information Base (MIB) is the collection of all objects managed by NMS. It defines attributes for the managed objects:

- Name
- Access authority
- Data type

The device-related statistic contents can be reached by accessing data items. Each proxy has its own MIB. MIB can be taken as an interface between NMS and Agent, through which NMS can read/write every managed object in Agent to manage and monitor the device.

MIB store information in a tree structure, its root is on the top, without name. Nodes of the tree are the managed objects, which take a uniquely path starting from root (OID) for identification. SNMP packets can access network devices by checking the nodes in MIB tree directory.

The A10E/A28E supports standard MIB and Orion customized MIB.

9.1.2 Preparing for configurations

Scenario

When you need to log in to the A10E/A28E through NMS, please configure SNMP basic functions for A10E/A28E in advance.

Prerequisite

- Configure the IP address of the SNMP interface.
- Configure the routing protocol and ensure that the route between the A10E/A28E and NMS is reachable.

9.1.3 Default configurations of SNMP

The default configuration of SNMP is as below.

Function	Default value												
SNMP view	system and internet views (default)												
SNMP community	public and private communities (default) <table border="1"> <thead> <tr> <th>Index</th> <th>CommunityName</th> <th>ViewName</th> <th>Permission</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>public</td> <td>internet</td> <td>ro</td> </tr> <tr> <td>2</td> <td>private</td> <td>internet</td> <td>rw</td> </tr> </tbody> </table>	Index	CommunityName	ViewName	Permission	1	public	internet	ro	2	private	internet	rw
Index	CommunityName	ViewName	Permission										
1	public	internet	ro										
2	private	internet	rw										
SNMP access group	initialnone and initial access groups (default)												
SNMP user	none, md5nopriv, and shanopriv users (default)												

Function	Default value																
Mapping relationship between SNMP user and access group	<table border="1"> <thead> <tr> <th>Index</th> <th>GroupName</th> <th>UserName</th> <th>SecModel</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>initialnone</td> <td>none</td> <td>usm</td> </tr> <tr> <td>1</td> <td>initial</td> <td>md5nopriv</td> <td>usm</td> </tr> <tr> <td>2</td> <td>initial</td> <td>shanopriv</td> <td>usm</td> </tr> </tbody> </table>	Index	GroupName	UserName	SecModel	0	initialnone	none	usm	1	initial	md5nopriv	usm	2	initial	shanopriv	usm
Index	GroupName	UserName	SecModel														
0	initialnone	none	usm														
1	initial	md5nopriv	usm														
2	initial	shanopriv	usm														
Logo and the contact method of administrator	support@orionnetworks.com																
Device physical location	usa orion																
Trap	Enable																
SNMP target host address	N/A																
SNMP engine ID	800022B603000E5E13D266																

9.1.4 Configuring basic functions of SNMP v1/v2c

To protect itself and prevent its MIB from unauthorized access, SNMP Agent proposes the concept of community. The management station in the same community must use the community name in all Agent operating. Otherwise, their requests will not be accepted.

The community name uses different SNMP string to identify different groups. Different communities can have read-only or read-write access authority. Groups with read-only authority can only query the device information, while groups with read-write authority can configure the device and query the device information.

SNMP v1/v2c uses the community name authentication scheme, and the SNMP packets which are inconsistent to the community name will be discarded.

Configure basic functions of SNMP v1/v2c for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# snmp-server view <i>view-name</i> <i>oid-tree</i> [<i>mask</i>] { excluded included }	(Optional) create SNMP view and configure MIB variable range. The default view is internet view. The MIB variable range contains all MIB variables below "1.3.6" node of MIB tree.
3	Alpha-A28E(config)# snmp-server community <i>community-name</i> [view <i>view-name</i>] { ro rw }	Create community name and configure the corresponding view and authority. Use default view internet if view <i>view-name</i> option is empty.

Step	Configuration	Description
4	Alpha-A28E(config)# snmp-server access group-name [read view-name] [write view-name] [notify view-name] { v1sm v2csm }	(Optional) create and configure SNMP v1/v2c access group.
5	Alpha-A28E(config)# snmp-server group group-name user user-name { v1sm v2csm usm }	(Optional) configure the mapping between users and access groups. SNMP v1/v2c can specify the group for the community, and configure the security model of the group. When the security model is v1sm or v2csm, the security level will automatically change to noauthnopriv.

9.1.5 Configuring basic functions of SNMP v3

SNMPV3 uses USM mechanism. USM comes up with the concept of access group. One or more users correspond to one access group. Each access group sets the related read, write, and notification views. Users in an access group have access authorities of this view. The access group of users, who send Get and Set requests, must have authorities corresponding to the requests. Otherwise, the requests will not be accepted.

As shown in Figure 9-2, to access the switch through SNMP v3, you should perform the following configurations:

- Configure users.
- Configure the access group of users.
- Configure the view authority of the access group.
- Create views.

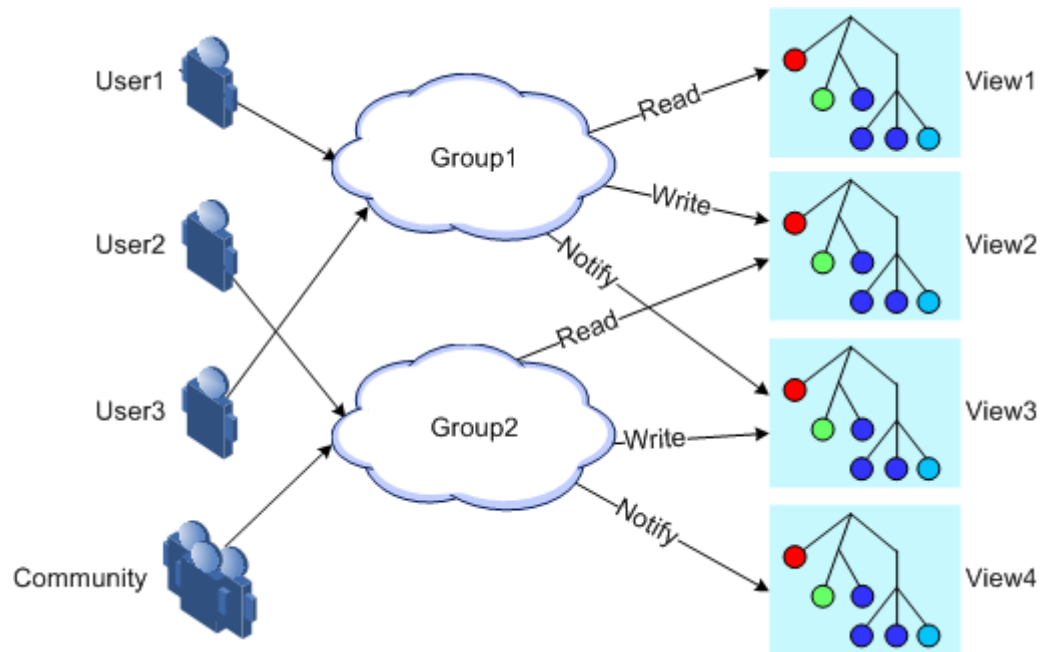


Figure 9-2 SNMP v3 authentication mechanism

Configure basic functions of SNMP v3 for the A10E/A28E as below.

Step	Configuration	Description
1	<code>Alpha-A28E#config</code>	Enter global configuration mode.
2	<code>Alpha-A28E(config)#snmp-server view view-name oid-tree [mask] { excluded included }</code>	(Optional) create SNMP view and configure MIB variable range.
3	<code>Alpha-A28E(config)#snmp-server user user-name [remote engine-id] [authentication { md5 sha } authpassword]</code>	Create users and configure authentication modes.
4	<code>Alpha-A28E(config)#snmp-server user user-name [remote engine-id] [authkey { md5 sha } keyword]</code>	(Optional) modify the authentication key and the encryption key.
5	<code>Alpha-A28E(config)#snmp-server access group-name [read view-name] [write view-name] [notify view-name] [context context-name { exact prefix }] usm { authnopriv noauthnopriv }</code>	Create and configure the SNMP v3 access group.
6	<code>Alpha-A28E(config)#snmp-server group group-name user user-name { usm v1sm v2csm }</code>	Configure the mapping relationship between users and the access group.


9.1.6 Configuring other information of SNMP

Other information of SNMP includes:

- Logo and contact method of the administrator, which is used to identify and contact the administrator
- Physical location of the device: describes where the device is located

SNMP v1, v2c, and v3 support configuring this information.

Configure other information of SNMP for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# snmp-server contact <i>contact</i>	(Optional) configure the logo and contact method of the administrator.  Note For example, set the E-mail to the logo and contact method of the administrator.
3	Alpha-A28E(config)# snmp-server location <i>location</i>	(Optional) specify the physical location of the device.

9.1.7 Configuring Trap



Trap configurations on SNMP v1, v2c, and v3 are identical except for Trap target host configurations. Please configure Trap as required.

Trap means the device sends unrequested information to NMS automatically, which is used to report some critical events.

Before configuring Trap, you need to perform the following configurations:

- Configure basic functions of SNMP. SNMP v1 and v2c need to configure the community name; SNMP v3 needs to configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the A10E/A28E and NMS is reachable.

Configure Trap of SNMP for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface ip <i>if-number</i>	Enter Layer 3 interface configuration mode.

Step	Configuration	Description
3	Alpha-A28E(config-ip)# ip address <i>ip-address</i> [<i>ip-mask</i>] <i>vlan-list</i>	Configure the IP address of the Layer 3 interface.
4	Alpha-A28E(config-ip)# exit	Exit from global configuration and enter privileged EXEC mode.
5	Alpha-A28E(config)# snmp-server host <i>ip-address</i> version 3 { authnopriv noauthnopriv } <i>user-name</i> [udpport <i>port-id</i>]	(Optional) configure SNMP v3-based Trap target host.
	Alpha-A28E(config)# snmp-server host <i>ip-address</i> version { 1 2c } <i>community</i> [udpport <i>udpport</i>]	(Optional) configure SNMP v1-/SNMP v2c-based Trap target host.
6	Alpha-A28E(config)# snmp-server enable traps	Enable Trap.

9.1.8 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show snmp access	Show SNMP access group configurations.
2	Alpha-A28E# show snmp community	Show SNMP community configurations.
3	Alpha-A28E# show snmp config	Show SNMP basic configurations, including local SNMP engine ID, ID and contact of the network management personnel, device location, and Trap switch status.
4	Alpha-A28E# show snmp group	Show the mapping relationship between SNMP users and the access group.
5	Alpha-A28E# show snmp host	Show Trap target host information.
6	Alpha-A28E# show snmp statistics	Show SNMP statistics.
7	Alpha-A28E# show snmp user	Show SNMP user information.
8	Alpha-A28E# show snmp view	Show SNMP view information.
9	Alpha-A28E# show snmp trap remote	Show remote Trap configurations of SNMP.

9.1.9 Example for configuring SNMP v1/v2c and Trap

Networking requirements

As shown in Figure 9-3, the route between the NView NNM system and Agent is reachable. The Nview NNM system can view MIBs in the view of the remote switch through SNMP v1/v2c. And the switch can automatically send Trap to Nview NNM in emergency.

By default, there is VLAN 1 in the A10E/A28E and all physical interfaces belong to VLAN 1.

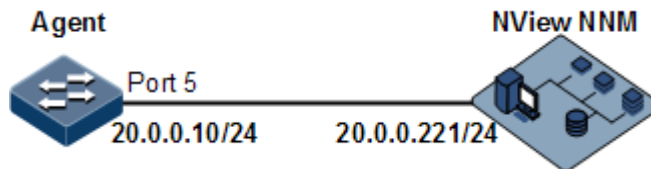


Figure 9-3 Configuring SNMP v1/v2c and Trap

Configuration steps

Step 1 Configure the IP address of the switch.

```
Alpha-A28E#config
Alpha-A28E(config)#interface ip 0
Alpha-A28E(config-ip)#ip address 20.0.0.10 255.255.255.0 1
Alpha-A28E(config-ip)#exit
```

Step 2 Configure the SNMP v1/v2c view.

```
Alpha-A28E(config)#snmp-server view mib2 1.3.6.1.2.1 included
```

Step 3 Configure the SNMP v1/v2c community.

```
Alpha-A28E(config)#snmp-server community orion view mib2 ro
```

Step 4 Configure Trap.

```
Alpha-A28E(config)#snmp-server enable traps
Alpha-A28E(config)#snmp-server host 20.0.0.221 version 2c orion
```

Checking results

Show IP address configurations by the command of **show interface ip**.

```
Alpha-A28E#show interface ip
Index      Ip Address      NetMask          Vid              Status      Mtu
-----
0          20.0.0.10      255.255.255.0   1                active      1500
```

Show view configurations by the command of **show snmp view**.

```
Alpha-A28E#show snmp view
Index:      0
View Name:  mib2
OID Tree:   1.2.6.1.2.1
Mask:       --
Type:       included

Index:      1
View Name:  system
OID Tree:   1.3.6.1.2.1.1
Mask:       --
Type:       included

Index:      2
View Name:  internet
OID Tree:   1.3.6
Mask:       --
Type:       included
```

Show community configurations by the command of **show snmp community**.

```
Alpha-A28E#show snmp community
Index  Community Name  View Name      Permission
-----
1      public          internet       ro
2      private         internet       rw
3      orion           mib2           ro
```

Show Trap target host configurations by the command of **show snmp host**.

```
Alpha-A28E#show snmp host
Index:          0
IP address:     20.0.0.221
Port:           162
User Name:      orion
SNMP Version:   v2c
Security Level: noauthnopriv
TagList:        bridge config interface rmon snmp ospf
```

9.1.10 Example for configuring SNMP v3 and Trap

Networking requirements

As shown in Figure 9-4, the route between the NView NNM system and Agent is reachable. The Nview NNM system monitors Agent through SNMP v3. And the Agent can automatically send Trap to Nview NNM in emergency.

By default, there is VLAN 1 in the A10E/A28E and all physical interfaces belong to VLAN 1.

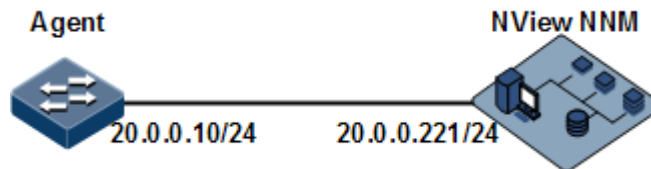


Figure 9-4 Configuring SNMP v3 and Trap

Configuration steps

Step 1 Configure the IP address of the switch.

```
Alpha-A28E#config
Alpha-A28E(config)#interface ip 0
Alpha-A28E(config-ip)#ip address 20.0.0.10 255.255.255.0 1
Alpha-A28E(config-ip)#exit
```

Step 2 Configure SNMP v3 access.

Configure access view mib2, including all MIB variables under 1.3.6.x.1.

```
Alpha-A28E(config)#snmp-server view mib2 1.3.6.1.2.1 1.1.1.1.0.1 included
```

Create user gusterus1. Adopt md5 authentication algorithm and set the password to orion.

```
Alpha-A28E(config)#snmp-server user guestuser1 authentication md5 orion
```

Create the guestgroup access group. Set the security mode to usm. Set the security level to authnopriv. Set the name of the read-only view to mib2.

```
Alpha-A28E(config)#snmp-server access guestgroup read mib2 usm authnopriv
```

Map user gudestuser1 to the access group guestgroup.

```
Alpha-A28E(config)#snmp-server group guestgroup user guestuser1 usm
```

Step 3 Configure Trap.

```
Alpha-A28E(config)#snmp-server enable traps  
Alpha-A28E(config)#snmp-server host 20.0.0.221 version 3 authnopriv  
guestuser1
```

Checking results

Show SNMP access group configurations by the command of **show snmp access**.

```
Index:          0  
Group:          initial  
Security Model: usm  
Security Level: authnopriv  
Context Prefix: --  
Context Match: exact  
Read View:      internet  
Write View:     internet  
Notify View:    internet  
  
Index:          1  
Group:          guestgroup  
Security Model: usm  
Security Level: authnopriv  
Context Prefix: --  
Context Match: exact  
Read View:      mib2  
Write View:     --  
Notify View:    internet  
  
Index:          2  
Group:          initialnone  
Security Model: usm  
Security Level: noauthnopriv  
Context Prefix: --  
Context Match: exact  
Read View:      system  
Write View:     --  
Notify View:    internet
```

Show the mapping relationship between users and the access group by the command of **show snmp group**.

```
Alpha-A28E#show snmp group  
Index  GroupName      UserName      SecMode1
```

0	initialnone	none	usm
1	initial	md5nopriv	usm
2	initial	shanopriv	usm
3	guestgroup	guestuser1	usm

Show Trap target host configurations by the command of **show snmp host**.

```
Alpha-A28E#show snmp host
Index:          0
IP address:    20.0.0.221
Port:         162
User Name:    guestuser1
SNMP Version: v3
Security Level: authnopriv
TagList:      bridge config interface rmon snmp ospf
```

9.2 KeepAlive

9.2.1 Introduction

KeepAlive packet is a kind of KeepAlive mechanism running in High-Level Data Link Control (HDLC) link layer protocol. The A10E/A28E will send a KeepAlive packet to confirm whether the peer is online every several seconds to realize neighbour detection mechanism.

Trap is the unrequested information sent by the A10E/A28E actively to NMS, used to report some urgent and important events.

The A10E/A28E sends KeepAlive Trap packet actively to the NView NNM system. The KeepAlive Trap packet includes the basic information of A10E/A28E, such as the name, OID, MAC address, and IP address. The Nview NNM system synchronizes device information based on IP address to discover NEs in a short time. This helps improve working efficiency and reduce working load of the administrator.

9.2.2 Preparing for configurations

Scenario

The A10E/A28E sends KeepAlive Trap packet actively to the NView NNM system. Therefore, the Nview NNM system can discover NEs in a short time. This helps improve working efficiency and reduce working load of the administrator. You can enable or disable the KeepAlive Trap and configure the period for sending KeepAlive Trap. When KeepAlive Trap is enabled, if configured with **snmp enable traps** and Layer 3 IP address, the A10E/A28E will send a KeepAlive Trap to all target hosts with Bridge Trap every KeepAlive Trap Interval.

Prerequisite

- Configure the IP address of the SNMP interface.
- Configure basic functions of SNMP. SNMP v1 and v2c need to configure the community name; SNMP v3 needs to configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the A10E/A28E and NMS is reachable.

9.2.3 Default configurations of KeepAlive

The default configuration of KeepAlive is as below.

Function	Default value
KeepAlive Trap	Disable
KeepAlive Trap period	300s

9.2.4 Configuring KeepAlive

Configure KeepAlive for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# snmp-server keepalive-trap enable	Enable KeepAlive Trap.
3	Alpha-A28E(config)# snmp-server keepalive-trap interval <i>period</i>	(Optional) configure the period for sending KeepAlive Trap.



Caution

To avoid multiple devices sending KeepAlive Trap at the same time according to the same period and causing heavy network management load, the real transmission period of KeepAlive Trap is timed as period+5s random transmission.

9.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show keepalive	View KeepAlive configurations.

9.2.6 Example for configuring KeepAlive

Networking requirements

Figure 9-5 shows how to configure KeepAlive.

- IP address of the switch: 192.169.1.2
- IP address of the SNMP v2c Trap target host: 192.168.1.1
- Name of the read-write community: public
- SNMP version: SNMP v2c
- Period for sending KeepAlive Trap: 120s
- KeepAlive Trap: enabled

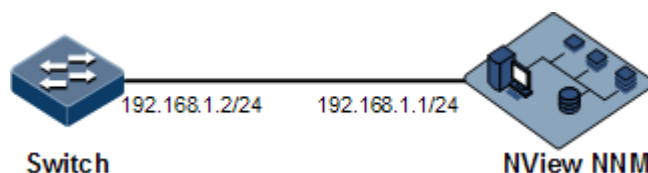


Figure 9-5 Configuring KeepAlive

Configuration steps

Step 1 Configure the management IP address of the switch.

```
Alpha-A28E#config
Alpha-A28E(config)#interface ip 0
Alpha-A28E(config-ip)#ip address 192.168.1.2 255.255.255.0 1
Alpha-A28E(config-ip)#exit
```

Step 2 Configure the IP address of the SNMP Trap target host.

```
Alpha-A28E(config)#snmp-server host 192.168.1.1 version 2c public
```

Step 3 Enable KeepAlive Trap.

```
Alpha-A28E(config)#snmp-server keepalive-trap enable
Alpha-A28E(config)#snmp-server keepalive-trap interval 120
```

Checking results

Show KeepAlive configurations by the command of **show keepalive**.

```
Alpha-A28E#show keepalive
Keepalive Admin State:Enable
Keepalive trap interval:120s
Keepalive trap count:1
```

9.3 RMON

9.3.1 Introduction

Remote Network Monitoring (RMON) is a standard stipulated by IETF (Internet Engineering Task Force) for network data monitoring through different network Agent and NMS.

RMON is achieved based on SNMP architecture, including the network management center and the Agent running on network devices. On the foundation of SNMP, increase the subnet flow, statistics, and analysis to achieve the monitoring to one network segment and the whole network, while SNMP only can monitor the partial information of a single device and it is difficult for it to monitor one network segment.

RMON Agent is commonly referred to as the probe program; RMON Probe can take the communication subnet statistics and performance analysis. Whenever it finds network failure, RMON Probe can report network management center, and describes the capture information under unusual circumstances so that the network management center does not need to poll the device constantly. Compared with SNMP, RMON can monitor remote devices more actively and more effectively, network administrators can track the network, network segment or device malfunction more quickly. This approach reduces the data flows between network management center and Agent, makes it possible to manage large networks simply and powerfully, and makes up the limitations of SNMP in growing distributed Internet.

RMON Probe data collection methods:

- Distributed RMON: network management center obtains network management information and controls network resources directly from RMON Probe through dedicated RMON Probe collection data.
- Embedded RMON: embed RMON Agent directly to network devices (such as switches) to make them with RMON Probe function. Network management center will collect network management information through the basic operation of SNMP and the exchange data information of RMON Agent.

The A10E/A28E adopts embedded RMON, as shown in Figure 9-6. The A10E/A28E implements RMON Agent. Through this function, the management station can obtain the overall flow, error statistics, and performance statistics of this network segment connected to the managed network device interface to a monitor the network segment.

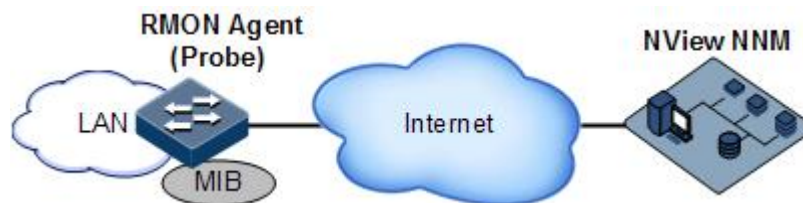


Figure 9-6 RMON

RMON MIBs are grouped into 9 groups according to functions. Currently, there are 4 groups achieved: statistics group, history group, alarm group, and event group.

- Statistics group: collect statistic information on each interface, including number of received packets and packet size distribution statistics.
- History group: similar with the statistics group, but it only collect statistic information in an assigned detection period.
- Alarm group: monitor an assigned MIB object, set the upper and lower thresholds in an assigned time interval, and trigger an event if the monitored object exceeds the threshold.
- Event group: cooperating with the alarm group, when alarm triggers an event, it records the event, such as sending Trap or writing it into the log, etc.

9.3.2 Preparing for configurations

Scenario

RMON helps monitor and account network traffics.

Compared with SNMP, RMON is a more high-efficient monitoring method. After you specifying the alarm threshold, the A10E/A28E actively sends alarms when the threshold is exceeded without gaining the variable information. This helps reduce the traffic of management and managed devices and facilitates managing the network.

Prerequisite

The route between the A10E/A28E and the NView NNM system is reachable.

9.3.3 Default configurations of RMON

The default configuration of RMON is as below.

Function	Default value
Statistics group	Enabled on all interfaces (including Layer 3 interfaces and physical interfaces)
History group	Disable
Alarm group	N/A
Event group	N/A

9.3.4 Configuring RMON statistics

RMON statistics is used to make statistics on an interface, including the number of received packets, undersized/oversized packets, collision, CRC and errors, discarded packets, fragments, unicast packets, broadcast packets, and multicast packets, as well as received packet size.

Configure RMON statistics for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# rmon statistics { ip <i>if-number</i> port-list <i>port-list</i> } [owner <i>owner-name</i>]	Enable RMON statistics on an interface and configure related parameters. By default, RMON statistics of all interfaces is enabled.



Note

When using the **no rmon statistics**{ **port-list** *port-list* | **ip** *if-number* } command to disable RMON statistics on an interface, you cannot continue to obtain the interface statistics, but the interface still can account data.

9.3.5 Configuring RMON historical statistics

Configure RMON historical statistics for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# rmon history { ip <i>if-number</i> port-list <i>port-list</i> } [shortinterval <i>short-period</i>] [longinterval <i>long-period</i>] [buckets <i>buckets-number</i>] [owner <i>owner-name</i>]	Enable RMON historical statistics on an interface and configure related parameters.



Note

When using the **no rmon history**{ **ip** *if-number* | **port-list** *port-list* } command to disable RMON historical statistics on an interface, the interface will not account data and clear all historical data collected previously.

9.3.6 Configuring RMON alarm group

You can monitor a MIB variable (mibvar) by setting a RMON alarm group instance (*alarm-id*). An alarm event is generated when the value of the monitored data exceeds the defined threshold. And then record the log or send Trap to the NView NNM system according to the definition of alarm events.

The monitored MIB variable must be real, and the data value type is correct.

- If the setting variable does not exist or value type variable is incorrect, return error.
- For the successfully-set alarm, if the variable cannot be collected later, close the alarm. Reset it if you need to monitor the variable again.

By default, the triggered event ID is 0, which indicates no event is triggered. If the number is not set to 0 and there is no event configured in the event group, the event is not successfully

triggered when the monitored variable is abnormal. The event cannot be successfully triggered unless the event is established.

The alarm will be triggered as long as the upper or lower threshold of the event in the event table is matched. The alarm is not generated even when alarm conditions are matched if the event related to the upper/lower threshold (*rising-event-id* or *falling-event-id*) is not configured in the event table.

Configure RMON alarm group for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# rmon alarm <i>alarm-id mibvar [interval</i> <i>period] { absolute delta }</i> rising-threshold <i>rising-value</i> <i>[rising-event-id] falling-</i> threshold <i>falling-value [falling-</i> <i>event-id] [owner owner-name]</i>	Add alarm instances to the RMON alarm group and configure related parameters.

9.3.7 Configuring RMON event group

Configure RMON event group for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# rmon event <i>event-id [log] [trap]</i> <i>[description string] [owner</i> <i>owner-name]</i>	Add events to the RMON event group and configure processing modes of events.

9.3.8 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show rmon	Show RMON configurations.
2	Alpha-A28E# show rmon alarms	Show RMON alarm group information.
3	Alpha-A28E# show rmon events	Show RMON event group information.
4	Alpha-A28E# show rmon statistics [<i>port port-id</i> <i> ip if-number</i>]	Show RMON statistics group information.
5	Alpha-A28E# show rmon history { <i>port port-id </i> <i>ip if-number</i> }	Show RMON history group information.

9.3.9 Maintenance

Maintain the A10E/A28E as below.

Command	Description
Alpha-A28E(config)# clear rmon	Clear all RMON configurations.

9.3.10 Example for configuring RMON alarm group

Networking requirements

As shown in Figure 9-7, the A10E/A28E is Agent, connecting to terminal through Console interface, connecting to remote NNM system through Internet. Enable RMON statistics and perform performance statistics on Port 3. When the number of packets received by Port 2 exceeds the threshold in a period, the A10E/A28E record logs and sends Trap alarm to the NView NNM system.

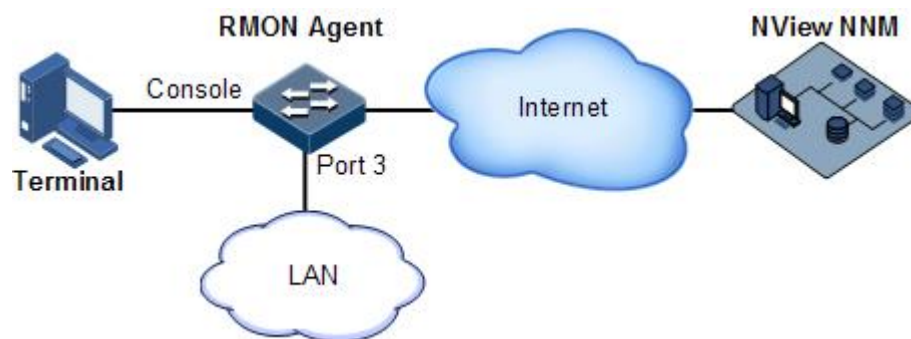


Figure 9-7 Configuring RMON alarm group

Configuration steps

- Step 1 Create event 1. Event 1 is used to record and send the log information which contains the string High-ifOutErrors. The owner of the log information is set to system.

```
Alpha-A28E#config
Alpha-A28E(config)#rmon event 1 log description High-ifOutErrors owner system
```

- Step 2 Create alarm 10. Alarm 10 is used to monitor the MIB variable (1.3.6.1.2.1.2.2.1.20.1) every 20 seconds. If the value of the variable is added by 15 or greater, a Trap is triggered. The owner of the Trap is also set to system.

```
Alpha-A28E(config)#rmon alarm 10 1.3.6.1.2.1.2.2.1.20.1 interval 20 delta rising-threshold 15 1 falling-threshold 0 owner system
```

Checking results

Check whether there is event group information on the device by the command of **show rmon alarms**.

```
Alpha-A28E#show rmon alarms
Alarm 10 is active, owned by system
Monitors 1.3.6.1.2.1.2.2.1.20.1 every 20 seconds
Taking delta samples, last value was 0
Rising threshold is 15, assigned to event 1
Falling threshold is 0, assigned to event 0
On startup enable rising and falling alarm
```

Check whether there is alarm group information on the device by the command of **show rmon events**.

```
Alpha-A28E#show rmon events
Event 1 is active, owned by system
Description is: High-ifOuterErrors.
Event generated at 0:0:0
Send TRAP when event is fired.
```

When an alarm event is triggered, you can view related records at the alarm management dialog box of the NView NNM system.

9.4 LLDP

9.4.1 Introduction

With the enlargement of network scale and increase of network devices, the network topology becomes more and more complex and network management becomes very important. A lot of network management software adopts "auto-detection" function to trace changes of network topology, but most of the software can only analyze to the 3rd layer and cannot make sure the interfaces connect to other devices.

Link Layer Discovery Protocol (LLDP) is based on IEEE 802.1ab standard. Network management system can fast grip the Layer 2 network topology and changes.

LLDP organizes the local device information in different Type Length Value (TLV) and encapsulates in Link Layer Discovery Protocol Data Unit (LLDPDU) to transmit to straight-connected neighbour. It also saves the information from neighbour as standard Management Information Base (MIB) for network management system querying and judging link communication.

Basic concepts

LLDP packet is to encapsulate LLDPDU Ethernet packet in data unit and transmitted by multicast.

LLDPDU is data unit of LLDP. The device encapsulates local information in TLV before forming LLDPDU, then several TLV fit together in one LLDPDU and encapsulated in Ethernet data for transmission.

As shown in Figure 9-9, LLDPDU is made by several TLV, including 4 mandatory TLV and several optional TLV.

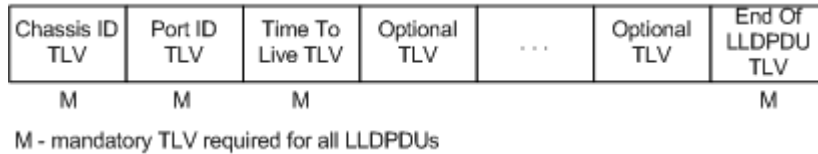


Figure 9-8 LLDPDU structure

TLV: unit combining LLDPDU, which refers to the unit describing the object type, length and information.

As shown in Figure 9-9, each TLV denotes piece of information at local, such as device ID, interface ID, etc. related Chassis ID TLV, Port ID TLV fixed TLV.

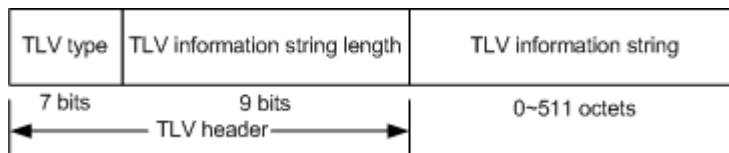


Figure 9-9 Basic TLV structure

TLV type value relationship is shown below; at present only types 0-8 are used.

Table 9-1 TLV type

TLV type	Description	Optional or required
0	End Of LLDPDU	Required
1	Chassis ID	Required
2	Port ID	Required
3	Time To Live	Required
4	Port Description	Optional
5	System Name	Optional
6	System Description	Optional
7	System Capabilities	Optional
8	Management Address	Optional

Working principles of LLDP

LLDP is a kind of point-to-point one-way issuance protocol, which notifies local device link status to peer end by sending LLDPDU (or sending LLDPDU when link status changes) periodically from local to peer end.

The procedure of packet exchange:

- When local device transmits packet, it gets system information required by TLV from NView NNM (Network Node Management) and gets configuration information from LLDP MIB to generate TLV and form LLDPDU to transmit to peer.
- The peer receives LLDPDU and analyzes TLV information. If there is any change, the information will be updated in neighbor MIB table of LLDP and notifies NView NNM system.

The aging time of Time To Live (TTL) of local device information in the neighbour node can be adjusted by modifying the parameter values of aging coefficient, sends LLDP packets to neighbour node, after receiving LLDP packets, neighbour node will adjust the aging time of its neighbour nodes (sending side) information. Aging time formula, $TTL = \text{Min} \{65535, (\text{interval} \times \text{hold-multiplier})\}$:

- Interval indicates the time period to send LLDP packets from neighbor node.
- Hold-multiplier refers to the aging coefficient of device information in neighbor node.

9.4.2 Preparing for configurations

Scenario

When you obtain connection information between devices through NView NNM system for topology discovery, the A10E/A28E needs to enable LLDP, notify their information to the neighbours mutually, and store neighbour information to facilitate the NView NNM system queries.

Prerequisite

N/A

9.4.3 Default configurations of LLDP

The default configuration of LLDP is as below.

Function	Default value
Global LLDP status	Disable
Interface LLDP status	Enable
Delay timer	2s
Period timer	30s
Aging coefficient	4
Restart timer	2s
LLDP alarm function status	Enable

Function	Default value
Alarm notification timer	5s

9.4.4 Enabling global LLDP



Caution

After global LLDP is disabled, you cannot re-enable it immediately. Global LLDP cannot be enabled unless the restart timer times out.

When you obtain connection information between devices through NView NNM system for topology discovery, the A10E/A28E needs to enable LLDP, notify their information to the neighbours mutually, and store neighbour information to facilitate the NView NNM system queries.

Enable global LLDP for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# lldp enable	Enable global LLDP. After global LLDP is enabled, use the lldp disable command to disable this function.

9.4.5 Enabling interface LLDP

Enable interface LLDP for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config- port)# lldp enable	Enable LLDP on an interface. Use the lldp disable command to disable this function.

9.4.6 Configuring basic functions of LLDP



Caution

When configuring the delay timer and period timer, the value of the delay timer should be smaller than or equal to a quarter of the period timer value.

Configure basic functions of LLDP for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# lldp message-transmission interval period	(Optional) configure the period timer of the LLDP packet.
3	Alpha-A28E(config)# lldp message-transmission delay period	(Optional) configure the delay timer of the LLDP packet.
4	Alpha-A28E(config)# lldp message-transmission hold-multiplier hold-multiplier	(Optional) configure the aging coefficient of the LLDP packet.
5	Alpha-A28E(config)# lldp restart-delay period	(Optional) restart the timer. When configuring the delay timer and period timer, the value of the delay timer should be smaller than or equal to a quarter of the period timer value.

9.4.7 Configuring LLDP alarm

When the network changes, you need to enable LLDP alarm notification function to send topology update alarm to the NView NNM system immediately.

Configure LLDP alarm for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# snmp-server lldp-trap enable	Enable LLDP alarm.
3	Alpha-A28E(config)# lldp trap-interval period	(Optional) configure the period timer of LLDP alarm Trap.



Note

After being enabled with LLDP alarm, the A10E/A28E sends Traps upon detecting aged neighbours, newly-added neighbours, and changed neighbour information.

9.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show lldp local config	Show LLDP local configurations.
2	Alpha-A28E# show lldp local system-data [port-list <i>port-id</i>]	Show LLDP local system information.
3	Alpha-A28E# show lldp remote [port-list <i>port-id</i>] [detail]	Show LLDP neighbor information.
4	Alpha-A28E# show lldp statistic [port-list <i>port-id</i>]	Show LLDP packet statistics.

9.4.9 Maintenance

Maintain the A10E/A28E as below.

No.	Command	Description
1	Alpha-A28E(config)# clear lldp statistic [port-list <i>port-id</i>]	Clear LLDP statistics.
2	Alpha-A28E(config)# clear lldp remote-table [port-list <i>port-id</i>]	Clear LLDP neighbor information.

9.4.10 Example for configuring basic functions of LLDP

Networking requirements

As shown in Figure 9-10, switches are connected to the NView NNM system. Enable LLDP on links between Switch A and Switch B. And then you can query the Layer 2 link changes through the NView NNM system. If the neighbour is aged, the neighbour is added, or the neighbour information changes, Switch A and Switch B sends LLDP alarm to the NView NNM system.

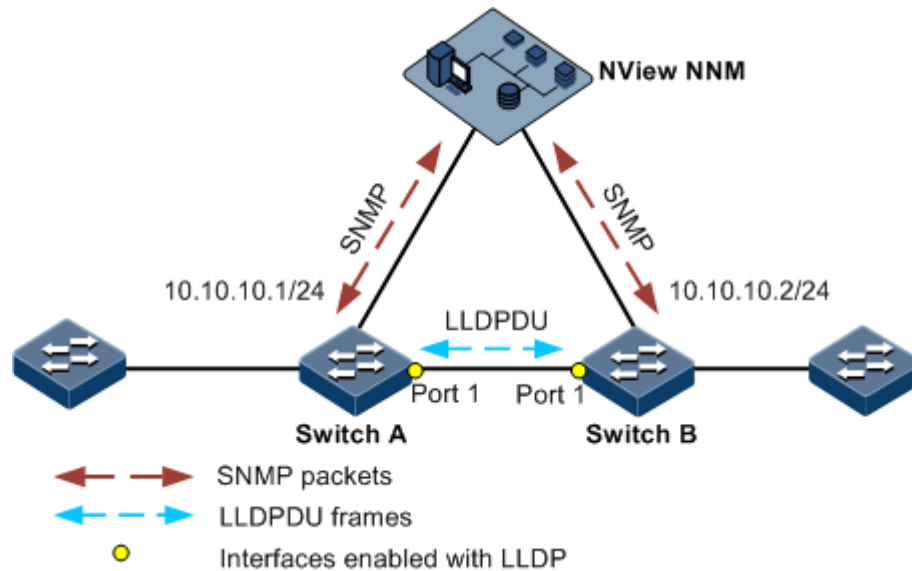


Figure 9-10 Configuring basic functions of LLDP

Configuration steps

Step 1 Enable LLDP globally and enable LLDP alarm.

Configure Switch A.

```
Alpha-A28E#hostname SwitchA
SwitchA#config
SwitchA(config)#lldp enable
SwitchA(config)#snmp-server lldp-trap enable
```

Configure Switch B.

```
Alpha-A28E#hostname SwitchB
SwitchB#config
SwitchB(config)#lldp enable
SwitchB(config)#snmp-server lldp-trap enable
```

Step 2 Configure management IP addresses.

Configure Switch A.

```
SwitchA(config)#create vlan 1024 active
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport access vlan 1024
SwitchA(config-port)#exit
SwitchA(config)#interface ip 1
SwitchA(config-ip)#ip address 10.10.10.1 1024
```

```
SwitchA(config-ip)#exit
```

Configure Switch B.

```
SwitchB(config)#create vlan 1024 active
SwitchB(config)#interface port-list 1
SwitchB(config-port)#switchport access vlan 1024
SwitchB(config)#interface ip 1
SwitchB(config-ip)#ip address 10.10.10.2 1024
SwitchB(config-ip)#exit
```

Step 3 Configure LLDP properties.

Configure Switch A.

```
SwitchA(config)#lldp message-transmission interval 60
SwitchA(config)#lldp message-transmission delay 9
SwitchA(config)#lldp trap-interval 10
```

Configure Switch B.

```
SwitchB(config)#lldp message-transmission interval 60
SwitchB(config)#lldp message-transmission delay 9
SwitchB(config)#lldp trap-interval 10
```

Checking results

Show local LLDP configurations by the command of **show lldp local config**.

```
SwitchA#show lldp local config
System configuration:
-----
LLDP enable status:enable (default is disabled)
LLDP enable ports:1-10
LldpMsgTxInterval:60 (default is 30s)
LldpMsgTxHoldMultiplier:4 (default is 4)
LldpReinitDelay:2 (default is 2s)
LldpTxDelay:9 (default is 2s)
LldpNotificationInterval:10 (default is 5s)
LldpNotificationEnable:enable (default is enabled)
```

```
SwitchB#show lldp local config
System configuration:
-----
```

```
LLDP enable status:enable (default is disabled)
LLDP enable ports:1
LldpMsgTxInterval:60 (default is 30s)
LldpMsgTxHoldMultiplier:4 (default is 4)
LldpReinitDelay:2 (default is 2s)
LldpTxDelay:9 (default is 2s)
LldpNotificationInterval:10 (default is 5s)
LldpNotificationEnable:enable (default is enabled)
```

Show LLDP neighbour information by the command of **show lldp remote**.

```
SwitchA#show lldp remote
Port  ChassisId          PortId      SysName  MgtAddress  ExpiredTime
-----
port1  000E.5E02.B010       port 1      SwitchB  10.10.10.2  106
.....
SwitchB#show lldp remote
Port  ChassisId          PortId      SysName  MgtAddress  ExpiredTime
-----
port1  000E.5E12.F120       port 1      SwitchA  10.10.10.1  106
```

9.5 Extended OAM

9.5.1 Introduction

Extended OAM is based on IEEE 802.3ah OAM links. Based on standard OAM extensibility, it enhances OAM functions, including remote configurations and monitoring.

As shown in Figure 9-11, establish an extended OAM link between the remote switch A and Central Office (CO) Switch B directly connected to the NView NNM system, to enable Switch B to manage Switch A.

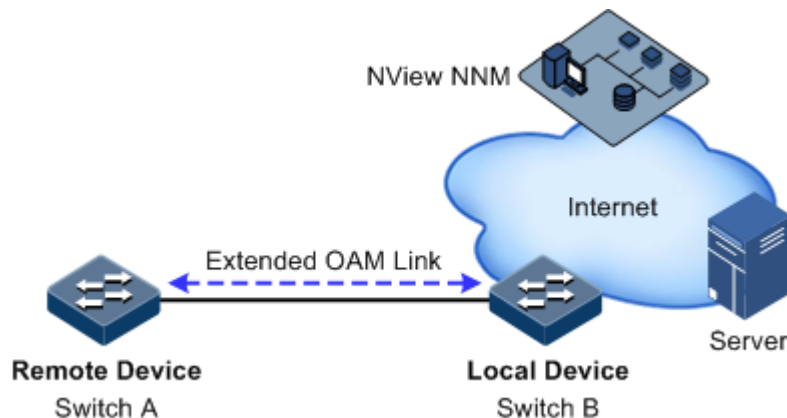


Figure 9-11 Extended OAM application networking

Extended OAM functions including remote configurations and monitoring, with details as below:

- Obtain attributes of the remote device: the CO device can obtain attributes, configurations, and statistics of the remote device through extended OAM.
- Configure basic functions for the remote device: through extended OAM, the CO device can configure some functions for the remote device, including host name, interface enabling/disabling status, rate, duplex mode, bandwidth, and failover status.
- Configure network management parameters for the remote device: the CO device can configure network management parameters for remote SNMP-supportive devices, such as IP address, gateway, management IP address, and read/write community, and then implement overall network management through SNMP.
- Support remote Trap: when an interface on a remote device is Up or Down, it sends an extended OAM notification to the CO device which will then send Trap message of the remote device to the NMS.
- Reboot the remote device: the CO device can send a command to reboot the remote device.
- Support other remote management functions: as the remote functions increase, the CO device can manage more remote functions through extended OAM protocols, such as SFP and QinQ.



Note

When the A10E/A28E works as the CO device, different remote devices may support different extended OAM functions. Whether an extended OAM function is supported depends on the remote device. For details, see the corresponding manuals.

For example, the remote device is the RC551E, which supports to be configured with the following extended OAM functions:

- Configure the IP address (including the default gateway and IP address of the out-of-band interface).
- Configure the name of the remote host.
- Configure network management of the remote device.
- Manage configuration files of the remote device.
- Reboot the remote device.
- Clear statistics of extended OAM links.
- Show extended OAM capabilities of the remote device.
- Show basic information about the remote device.
- Show interface information about the remote device.
- Show Trap function status of the remote device.
- Show extended OAM link status.

9.5.2 Preparation for configuration

Scenario

Extended OAM is mainly used to establish connection between Central Office (CO) device and remote device so as to achieve remote management.

Prerequisite

You need to complete the following tasks before configure extended OAM:

- Establish OAM link between devices to establish extended OAM link.

The following configurations take A10E/A28E as the CO device. For different remote devices, the extended OAM networking situation and configuration commands may be different; please take configuration according to the specific remote networking situation.

9.5.3 Default configurations of extended OAM

The default configuration of extended OAM is as below.

Function	Default value
OAM function status	Disable
OAM working mode	passive
Remote Trap function status	Enable

9.5.4 Establishing OAM link



Note

You need to establish OAM link between devices to establish extended OAM link and both sides of devices are OAM active mode and passive mode respectively.

Establish OAM link on CO device and remote device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# oam { active passive }	Configure OAM working mode. Establish both sides of OAM link; configure CO device as active mode and remote device as passive mode.
3	Alpha-A28E(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
4	Alpha-A28E(config- port)# oam enable	Enable interface OAM function.

9.5.5 Configure extended OAM protocols

Configure the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# extended-oam config-request enable	Enable power-on configuration request.
3	Alpha-A28E(config)# extended-oam notification enable	Enable sending extended OAM notification packet.

9.5.6 Entering remote configuration mode



Note

The interface can enter remote configuration mode only when OAM link is established between CO device and remote device.

Take the following configuration on CO device.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# remote-device	Enter remote configuration mode.
4	Alpha-A28E(config-remote)# interface client <i>client-id</i> Alpha-A28E(config-remoteport)#	(Optional) enter remote interface configuration mode.

9.5.7 (Optional) showing remote extended OAM capacity



Caution

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

On the CO device, you can use the command of **show oam capability** to show remote device extended OAM capacity, and then take configuration according to the specific device.

Configure the CO device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.

Step	Configuration	Description
3	Alpha-A28E(config-port)# remote-device	Enter remote configuration mode.
4	Alpha-A28E(config-remote)# show oam capability	Show remote device extended OAM management capacity.

9.5.8 Configuring remote host name



Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure the CO device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# remote-device	Enter remote configuration mode.
4	Alpha-A28E(config-remote)# hostname <i>hostname</i>	Configure remote host name.

9.5.9 Configuring MTU for the remote device



Caution

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure the remote device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# remote-device	Enter remote configuration mode.
4	Alpha-A28E(config-remote)# system mtu <i>size</i>	Configure MTU for the remote device.

9.5.10 Configuring the IP address of the remote device



Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure the remote device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config- port)# remote-device	Enter remote configuration mode.
4	Alpha-A28E(config- remote)# ip address <i>ip-</i> <i>address</i> [<i>ip-mask</i>] <i>vlan-list</i>	Configure remote device IP address. Set the IP address of IP interface 0 on the remote device to take effect. IP address configuration needs to specify management VLAN, if this VLAN does not exist, create VLAN and take all interfaces as member interface by default; if associated VLAN exists, do not modify the member interface configuration.
5	Alpha-A28E(config- remote)# ip default- gateway <i>ip-address</i>	(Optional) configure remote device default gateway. The default gateway and configured IP address of IP interface 0 need to be in the same network segment.

9.5.11 Configuring interface parameters on the remote device



Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.


Configure different remote interface parameters in different mode:

- In remote interface configuration mode, configure remote interface Up/Down, speed and working mode, etc.
- In remote configuration mode, configure remote interface auto-negotiation, interface bandwidth, and failover, etc.

Configuring interface parameters in remote interface configuration mode

In remote interface configuration mode, configure remote interface Up/Down, speed and working mode, etc.

Configure the CO device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config- port)# remote-device	Enter remote configuration mode.
4	Alpha-A28E(config- remote)# interface client <i>client-id</i>	Enter remote interface configuration mode.
5	Alpha-A28E(config- remoteport)# shutdown	(Optional) shut down remote interface.
6	Alpha-A28E(config- remoteport)# speed { auto 10 100 }	(Optional) configure remote device Client interface speed.
7	Alpha-A28E(config- remoteport)# duplex { full half }	(Optional) configure remote device Client interface duplex mode.  Note The OAM link maybe disconnect after configuring remote interface duplex mode.
8	Alpha-A28E(config- remoteport)# flowcontrol { on off }	(Optional) enable/disable flow control on the user interface of the remote device.

Configuring interface parameters in remote configuration mode

In remote configuration mode, configure remote interface auto-negotiation, interface bandwidth, and failover, etc.

Configure the CO device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config- port)# remote-device	Enter remote configuration mode.
4	Alpha-A28E(config- remote)# description { line <i>line-id</i> client <i>client-id</i> } <i>string</i>	(Optional) configure description of the interface on the remote device.

Step	Configuration	Description
5	Alpha-A28E(config-remote)# line-speed auto	(Optional) configure rate auto-negotiation on the Line interface of the remote device. You can configure the optical interface with auto-negotiation when the interface connecting remote device and CO device is 1000 Mbit/s optical port.
6	Alpha-A28E(config-remote)# rate-limit <i>interface-type</i> <i>interface-number</i> ingress rate	(Optional) configure remote ingress interface bandwidth.
7	Alpha-A28E(config-remote)# fault-pass enable	(Optional) enable remote failover. The fault optical interface on the remote device changes to electrical port after being enabled with remote failover.
8	Alpha-A28E(config-remote)# inside-loopback [crc-recalculate]	(Optional) enable inner loopback on the optical interface on the remote device.
9	Alpha-A28E(config-remote)# test cable-diagnostics	Conduct virtual line detection on the remote device.



Note

For the above interface configuration in remote configuration mode:

- If the command line provides specified interface parameters, the corresponding configuration will take effect on specified interface;
- If the command line does not provide specified interface parameters, the corresponding configuration will take effect on all interfaces of the corresponding type on the remote device.

9.5.12 Uploading and downloading files on the remote device

Downloading files from the server to the remote device

The system bootstrap file, system startup file, configuration files, and FPGA file can be forwarded from the CO device to the remote device, which can be initiated by the CO device or the remote device. If the CO device initiates this, it can upgrade multiple remote devices.

On the CO device, download files from the FTP/TFTP server to the remote device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# remote-device	Enter remote configuration mode.

Step	Configuration	Description
4	Alpha-A28E(config-remote)# download { bootstrap startup-config system-boot fpga } { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	On the CO device, download files from the FTP/TFTP server to the remote device.

On the remote device, download files from the FTP/TFTP server to the remote device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# download { bootstrap startup-config system-boot fpga } { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	On the remote device, download files from the FTP/TFTP server to the remote device.

Uploading files from the remote device to the server

The system bootstrap file, system startup file, configuration files, and FPGA file can be forwarded from the remote device to the server, which can be initiated by the CO device or the remote device. If the CO device initiates this, it cannot upgrade multiple remote devices.

On the CO device, upload files from the remote device to the server as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# remote-device	Enter remote configuration mode.
4	Alpha-A28E(config-remote)# upload { startup-config system-boot } { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	On the CO device, upload files from the remote device to the server.

On the remote device, upload files from the remote device to the server as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# upload { startup-config system-boot } { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	On the remote device, upload files from the remote device to the server.

Downloading remote device files from the server to the CO device

The system bootstrap file, system startup file, configuration files, and FPGA file of the remote device can be downloaded through FTP or TFTP from the server to the CO device, and saved with a specified name in the flash of the remote device. This is prepared for further upgrading of the remote device.

Download remote device files from the server to the CO device as below.

Step	Configuration	Description
1	Alpha-A28E# download { remote-bootstrap remote-system-boot remote-startup-config remote-fpga } { ftp <i>ip-address user-name password file-name local-file-name</i> tftp <i>ip-address file-name local-file-name</i> }	Download remote device files from the server to the CO device.

Uploading remote device files from the CO device to the server

Upload remote device files from the CO device to the server as below.

Step	Configuration	Description
1	Alpha-A28E# upload { remote-bootstrap remote-system-boot remote-startup-config remote-fpga } { ftp <i>ip-address user-name password file-name local-file-name</i> tftp <i>ip-address file-name local-file-name</i> }	Upload remote device files from the CO device to the server.

Downloading files from the CO device to the remote device

The remote device files saved in the flash of the CO device can be downloaded to the remote device through extended OAM protocols, which can be initiated by the CO device or the remote device. If the CO device initiates this, it can upgrade multiple remote devices.

On the CO device, download files from the CO device to the remote device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config- port)# remote-device	Enter remote configuration mode.
4	Alpha-A28E(config- remote)# download { bootstrap system-boot fpga } <i>file-name</i>	Download the system bootstrap file, system startup file, and FPGA file from the CO device to the remote device.
5	Alpha-A28E(config- remote)# download startup-config [<i>file-name</i>]	Download configuration files from the CO device to the remote device.

On the remote device, download files from the CO device to the remote device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config- port)# download { bootstrap system-boot fpga } <i>file-name</i>	Download the system bootstrap file, system startup file, and FPGA file from the CO device to the remote device.
4	Alpha-A28E(config- port)# download startup-config [<i>file-name</i>]	Download configuration files from the CO device to the remote device.

9.5.13 Configuring remote network management



Caution

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configuring remote network management

Configure the CO device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config- port)# remote-device	Enter remote configuration mode.

Step	Configuration	Description
4	Alpha-A28E(config-remote)#snmp-server community <i>community-name</i> { ro rw }	Configure remote read/write community and read/write authority.

Configuring remote Trap

The remote device generates Trap information, which will be sent to CO device through OAM notification packet and then CO device will send the Trap to network management system.

To configure network management system to accept remote Trap, you need to enable remote Trap function on CO device and maybe enable to send extended OAM notification function on remote device.

Configure the CO device as below.

Step	Configuration	Description
1	Alpha-A28E#config	Enter global configuration mode.
2	Alpha-A28E(config)#snmp trap remote enable	Enable remote device to send Trap function.



Note

To configure remote Trap, some remote devices need to perform the command of **extended-oam notification enable** to enable to send extended OAM notification function in remote configuration mode.

9.5.14 Configuring remote VLAN



Caution

- Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.
- Different remote devices may have different configuration commands.

You can configure remote VLAN and deal with packets received by the remote device according to VLAN property configuration, such as set remote VLAN status, VLAN tag property and create remote VLAN group, etc.

Remote VLAN status:

- **dot1q**: remote VLAN mode is Dot1q; the packets entering device interface will be forwarded in accordance with dot1q mode.
- **forbid**: forbid remote VLAN function; the packets entering device interface will be forwarded in accordance with transparent transmission mode.
- **port**: remote VLAN is Port mode.

Enable remote VLAN CoS function, deal with the packets entering device interface according to VLAN priority, high priority first and low priority second.

Configure the CO device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config- port)# remote-device	Enter remote configuration mode.
4	Alpha-A28E(config- remote)# vlan { dot1q forbid port }	(Optional) configure remote VLAN status.
5	Alpha-A28E(config- remote)# vlan cos enable	(Optional) enable remote VLAN CoS.
6	Alpha-A28E(config- remote)# vlan { cable-port cpu-port fiber-port } { tag untag } priority <i>priority pvid pvid</i>	(Optional) configure remote VLAN tag property.
7	Alpha-A28E(config- remote)# vlan group <i>group-id vid vid member-list member-list</i>	(Optional) create remote VLAN group.

9.5.15 Configuring remote QinQ



Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure the CO device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config- port)# remote-device	Enter remote configuration mode.
4	Alpha-A28E(config- remote)# switch-mode transparent	(Optional) configure remote device to work in full transparent transmission mode.
5	Alpha-A28E(config- remote)# switch-mode dot1q-vlan native-vlan <i>vlan-id [line]</i>	(Optional) enable remote device to work single Tag forwarding mode.

Step	Configuration	Description
6	Alpha-A28E(config-remote)# switch-mode double-tagged-vlan [<i>tpid tpid</i>] native-vlan <i>vlan-id</i> [line]	(Optional) configure remote device to work in double Tag forwarding mode.

 **Note**

- To configure remote device to work in full transparent transmission mode, do not deal with data packets.
- To configure remote device to work in single Tag mode, after the A10E/A28E is configured to single Tag mode, the data packets without Tag from user interface will be marked with Tag with local VLAN ID; do nothing if there is Tag.
- To configure remote device to work in double Tag mode, after the A10E/A28E is configured to double Tag mode, the data packets without Tag from user interface will be marked with outer Tag with specified TPID and local VLAN ID.

9.5.16 Managing remote configuration files

 **Note**

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure the CO device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# remote-device	Enter remote configuration mode.
4	Alpha-A28E(config-remote)# write	(Optional) save remote device configuration files in remote device flash.
5	Alpha-A28E(config-remote)# write local	(Optional) save remote device configuration files in CO device flash.
6	Alpha-A28E(config-remote)# erase	(Optional) delete remote device configuration files.

9.5.17 Rebooting remote device



Note

- During resetting or rebooting remote device, OAM link maybe disconnect and the CO device will not connect with remote device.
- Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure the CO device as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface port port-id	Enter physical layer interface configuration mode.
3	Alpha-A28E(config-port)# remote-device	Enter remote configuration mode.
4	Alpha-A28E(config-remote)# reboot	Reboot remote device.

9.5.18 Checking configuration



Note

Whether the remote device supports the following items varies with the specific remote device. For details, see the corresponding manuals.

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E(config-remote)# show remote-device information	Show basic information about the remote device.
2	Alpha-A28E# show extended-oam status [port-list port-list]	Show extended OAM link status.
3	Alpha-A28E(config-remote)# show interface port [detail statistics]	Show information about the remote device interfaces.
4	Alpha-A28E(config-remote)# show cable-diagnostics	Show information about line diagnosis.
5	Alpha-A28E(config-remote)# show inside-loopback	Show loopback status on the optical interface on the remote device and loopback parameters.
6	Alpha-A28E(config-remote)# show oam capability	Show OAM capabilities supported by the remote device.
7	Alpha-A28E(config-remote)# show remote-device information	Show basic information about the remote device.

No.	Item	Description
1	Alpha-A28E(config-remote)# show remote-device information	Show basic information about the remote device.
2	Alpha-A28E# show extended-oam status [port-list port-list]	Show extended OAM link status.
8	Alpha-A28E(config-remote)# show vlan basic-information	Show basic information about VLANs on the remote device.
9	Alpha-A28E(config-remote)# show vlan group-information { all group-id }	Show information about VLAN groups on the remote device.
10	Alpha-A28E# show extended-oam statistics [port-list port-list]	Show statistics of extended OAM frames.
11	Alpha-A28E# show snmp trap remote	Show Trap enabling status on the remote device.

9.5.19 Maintenance

Maintain the A10E/A28E as below.

Item	Description
Alpha-A28E(config)# clear extended-oam statistics [port-list port-list]	Clear statistics of extended OAM packets.

9.5.20 Example for configuring extended OAM to manage the remote device

Networking requirements

As shown below, the RC551E is connected to the switch. Configured with extended OAM, the switch can remotely manage the RC551E. Configure the host name and IP address of the RC551E on the switch.

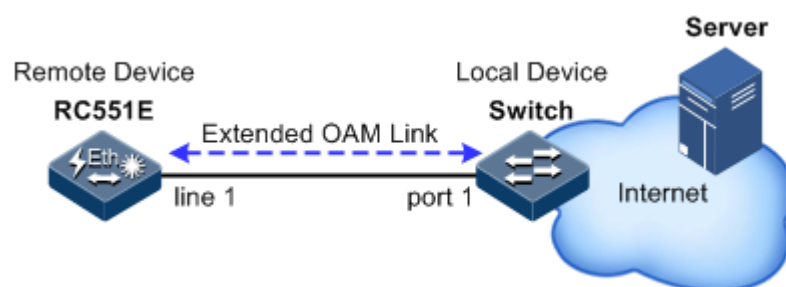


Figure 9-12 Configuring extended OAM to manage the remote device

Configuration steps

Step 1 Establish an OAM link between the RC551E and the switch.

Set the RC551E to work in OAM passive mode, and enable OAM.

```
Alpha-A28E#hostname RC55x
RC55x#config
RC55x(config)#oam passive
RC55x(config)#interface line 1
RC55x(config-port)#oam enable
```

Set the switch to work in OAM active mode, and enable OAM.

```
Alpha-A28E#hostname Switch
Switch#config
Switch(config)#oam active
Switch(config)#interface port 1
Switch(config-port)#oam enable
```

Step 2 Configure the host name and IP address of the RC551E on the switch.

```
Switch(config-port)#remote-device
Switch(config-remote)#hostname RC551E
Switch(config-remote)#ip address 192.168.18.100 255.255.255.0 200
```

Checking result

Show configurations of the remote device on the switch.

```
Alpha-A28E(config-remote)#show remote-device information
Local port:port1
Product Name:                RC551E-4GEF
Hostname:                    RC551E
Operation Software Version:   ROS_4.14.1670.RC551E-
4GEF.39.20110914
Hardware Version:            Hardware RC551E-4GEF
Main chip id:                N/A
Total ports:                 6
FPGA chip id:                N/A
FPGA soft version:           N/A
IP Address/mask:              192.168.18.100/255.255.255.0
IP Interface vlan:            0
Vlan member Port:
Untag port:
IP Default-gateway:           0.0.0.0
OutBand-port IP/Mask:         N/A/N/A
```


Community Name/Access:	N/A/N/A
OAM Notification:	
Device current temperature(Celsius):	0(Celsius)
Device voltage:	low
Ref. volt(mv)	Current volt(mv)
3300	01
2500	01
1800	01
1200	01

9.6 Optical module DDM

9.6.1 Introduction

Digital Diagnostic Monitoring (DDM) on the A10E/A28E supports diagnosing the Small Form-factor Pluggable (SFP) module.

SFP DDM provides a method for monitoring performance. By analyzing monitored data provides by the SFP module, the administrator can predict the lifetime for the SFP module, isolate system faults, as well as verify the compatibility of the SFP module.

The SFP module offers 5 performance parameters:

- Module temperature
- Internal Power Feeding Voltage (PFV)
- Launched bias current
- Launched optical power
- Received optical power

When SFP performance parameters exceed thresholds or when SFP state changes, related Trap is generated.

9.6.2 Preparing for configurations

Scenario

SFP DDM provides a method for monitoring performance parameters of the SFP module. By analyzing monitored data, you can predict the lifetime for the SFP module, isolate system faults, as well as verify the compatibility of the SFP module.

Prerequisite

N/A

9.6.3 Default configurations of optical module DDM

The default configuration of optical module DDM is as below.

Function	Default value
Optical module DDM	Disable
Optical module DDM sending Trap function status	Enable

9.6.4 Enabling optical module DDM

Enable optical module DDM for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# transceiver digitaldiagnostic enable	Enable optical module DDM.

9.6.5 Enabling optical module DDM to send Trap messages

Enable optical module DDM to send Trap messages for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# snmp trap transceiver enable	Enable optical module DDM to send Trap messages.

9.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show interface port [port-id] transceiver [detail]	Show configurations of optical module DDM.
2	Alpha-A28E# show interface port [port-id] transceiver [detail] threshold-violations	Show performance parameters and thresholds of optical module DDM.
3	Alpha-A28E# show interface port [port-id] transceiver information	Show information about the optical module DDM.

9.7 System log

9.7.1 Introduction

The system log refers that the device records the system information and debugging information in a log and sends the log to the specified destination. When the device fails to work, you can check and locate the fault easily.

The system information and some scheduling output will be sent to the system log to deal with. According to the configuration, the system will send the log to various destinations. The destinations that receive the system log are divided into:

- Console: send the log message to the local console through Console interface.
- Host: send the log message to the host.
- Monitor: send the log message to the monitor, such as Telnet terminal.
- File: send the log message to the Flash of the device.

The system log is usually in the following format:

```
timestamp module-level- Message content
```

The following is an example of system log content.

```
FEB-22-2005 14:27:33 CONFIG-7-CONFIG:USER "admin" Run "logging on"  
FEB-22-2005 06:46:20 CONFIG-6-LINK_D:port 2 Link Down  
FEB-22-2005 06:45:56 CONFIG-6-LINK_U:port 2 Link UP
```

The format for outputting to the logging server is as below:

```
timestamp module-level- Message content
```

The following is an example of log content for the logging server.

```
07-01-200811:31:28Local0.Debug20.0.0.6JAN 01 10:22:15 ISCOM2110: CONFIG-  
7-CONFIG:USER " admin " Run " logging on "  
07-01-200811:27:41Local0.Debug20.0.0.6JAN 01 10:18:30 ISCOM2110: CONFIG-  
7-CONFIG:USER " admin " Run " ip address 20.0.0.6 255.0.0.0 1 "
```

According to the severity level, the log is identified by 8 severity levels, as listed in Table 9-2.

Table 9-2 Log level

Severity	Level	Description
Emergency	0	The system cannot be used.

Severity	Level	Description
Alert	1	Need to deal immediately.
Critical	2	Serious status
Error	3	Errored status
Warning	4	Warning status
Notice	5	Normal but important status
Informational	6	Informational event
Debug	7	Debugging information



Note

The severity of output information can be manually set. When you send information according to the configured severity, you can just send the information whose severity is less than or equal to that of the configured information. Such as, when the information is configured with the level 3 (or the severity is errors), the information whose level ranges from 0 to 3, that is, the severity ranges from emergencies to errors, can be sent.

9.7.2 Preparing for configurations

Scenario

The A10E/A28E generates critical information, debugging information, or error information of the system to system logs and outputs the system logs to log files or transmit them to the host, Console interface, or monitor for viewing and locating faults.

Prerequisite

N/A

9.7.3 Default configurations of system log

The default configuration of system log is as below.

Function	Default value
System log	Enable
Output log information to Console	Enable, the default level is information (6).
Output log information to host	N/A, the default level is information (6).
Output log information to file	Disable, the fixed level is warning (4).
Output log information to monitor	Disable, the default level is information (6).
Log Debug level	low

Function	Default value
Transmitting rate of system log	No limit

9.7.4 Configuring basic information of system log

Configure basic information of system log for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# logging on	(Optional) Enable system log.
3	Alpha-A28E(config)# logging time-stamp { date-time null relative-start }	(Optional) configure timestamp for system log.
4	Alpha-A28E(config)# logging rate log-num	(Optional) configure transmitting rate of system log.

9.7.5 Configuring system log output

Configure system log output for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# logging console { log-level alerts critical debugging emergencies errors informational notifications warnings }	(Optional) output system logs to the Console.
3	Alpha-A28E(config)# logging host ip-address { local0 local1 local2 local3 local4 local5 local6 local7 } { log-level alerts critical debugging emergencies errors informational notifications warnings }	(Optional) output system logs to the log server. Up to 10 log servers are supported.
4	Alpha-A28E(config)# logging monitor { log-level alerts critical debugging emergencies errors informational notifications warnings }	(Optional) output system logs to the monitor.

Step	Configuration	Description
5	Alpha-A28E(config)# logging file	(Optional) output system logs to the Flash of the A10E/A28E. Only warning-level logs are available.

9.7.6 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show logging	Show system log configurations.
2	Alpha-A28E# show logging file	Show system log contents.

9.7.7 Example for outputting system logs to log server

Networking requirements

As shown in Figure 9-13, configure system log to output system logs of the switch to the log server, facilitating view them at any time.

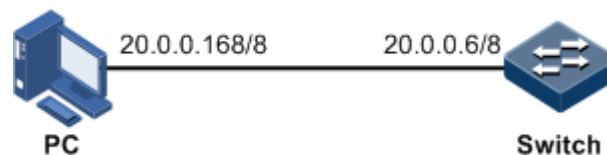


Figure 9-13 Outputting system logs to log servers

Configuration steps

Step 1 Configure the IP address of the switch.

```
Alpha-A28E#config
Alpha-A28E(config)#interface ip 0
Alpha-A28E(config-ip)#ip address 20.0.0.6 255.0.0.0 1
Alpha-A28E(config-ip)#exit
```

Step 2 Output system logs to the log server.

```
Alpha-A28E(config)#logging on
Alpha-A28E(config)#logging time-stamp date-time
```

```
Alpha-A28E(config)#logging rate 2
Alpha-A28E(config)#logging host 20.0.0.168 local3 warnings
```

Checking results

Show system log configurations by the command of **show logging**.

```
Alpha-A28E#show logging
Syslog logging:Enable, 0 messages dropped, messages rate-limited 2 per
second
Console logging:Enable, level=informational, 19 Messages logged
Monitor logging:Disable, level=informational, 0 Messages logged
Time-stamp logging messages: date-time
```

```
Log host information:
Target Address      Level           Facility        Sent    Drop
-----
20.0.0.168         warnings        local3          0       0
```

9.8 Power monitoring

9.8.1 Introduction

The A10E/A28E supports monitoring power alarm, namely, Dying Gasp alarm.

9.8.2 Preparing for configurations

Scenario

You can configure the power alarm function to monitor faults. When the power is abnormal, the system generates the Syslog or sends Trap message, informing you to take actions accordingly to avoid power failure.

Prerequisite

N/A

9.8.3 Default configurations of power monitoring

Configure the A10E/A28E as below.

Function	Description
Power alarm Trap sending status	Enable

9.8.4 Configuring power monitoring alarm

Configure power monitoring alarm for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# alarm power	Enable sending power alarm Trap.

9.8.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show alarm power	Show power alarm status.

9.9 CPU monitoring

9.9.1 Introduction

The A10E/A28E supports CPU monitoring. It can monitor state, CPU utilization, and stack usage in real time. It helps to locate faults.

CPU monitoring can provide the following functions:

- View CPU utilization

It can be used to view CPU unitization in each period (5s, 1 minute, 10 minutes, and 2 hours). Total CPU unitization in each period can be shown dynamically or statically.

It can be used to view the operating status of all tasks and the detailed running status of assigned tasks.

It can be used to view history CPU utilization in each period.

It can be used to view death task information.

- CPU unitization threshold alarm

If system CPU utilization changes below lower threshold or above upper threshold in a specified sampling period, an alarm will be generated and a Trap message will be sent. The Trap message provides serial number and CPU utilization of 5 tasks whose CPU unitization is the highest in the latest period (5s, 1 minute, 10 minutes).

9.9.2 Preparing for configurations

Scenario

CPU monitoring can monitor state, CPU utilization, and stack usage in real time, provide CPU utilization threshold alarm, detect and eliminate hidden dangers, or help administrator for fault location.

Prerequisite

Before configuring CPU monitoring, you need to perform the following operation:

- When the CPU monitoring alarm needs to be output in Trap mode, configure Trap output target host address, which is IP address of NView NNM system.

9.9.3 Default configurations of CPU monitoring

The default configuration of CPU monitoring is as below.

Function	Default value
CPU utilization rate alarm Trap output	Disable
Upper threshold of CPU utilization alarm	100%
Lower threshold of CPU utilization alarm	1%
Sampling period of CPU utilization	60s

9.9.4 Viewing CPU monitoring information

View CPU monitoring information for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# show cpu-utilization [dynamic history { 10min 1min 2hour 5sec }]	View CPU utilization.
2	Alpha-A28E# show process [dead sorted { normal-priority process-name } taskname]	View states of all tasks.
3	Alpha-A28E# show process cpu [sorted [10min 1min 5sec invoked]]	View CPU utilization of all tasks.

9.9.5 Configuring CPU monitoring alarm

Configure CPU monitoring alarm for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.

Step	Configuration	Description
2	Alpha-A28E(config)# snmp-server traps enable cpu-threshold	Enable CPU threshold alarm Trap.
3	Alpha-A28E(config)# cpu rising-threshold rising-threshold-value [falling-threshold falling-threshold-value] [interval interval-value]	(Optional) configure CPU alarm upper threshold, lower threshold, and sampling interval. The upper threshold must be greater than the lower threshold. After CPU threshold alarm Trap is enabled, the system will automatically send a Trap message if the CPU utilization changes below lower threshold or above upper threshold in a specified sampling period.

9.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Alpha-A28E# show cpu-utilization	Show CPU utilization and related configurations.

9.10 Ping

Configure Ping for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# ping ip-address [count count] [size size] [waittime period]	(Optional) test the connectivity of the IPv4 network by the ping command.



Note

The A10E/A28E cannot carry out other operations in the process of executing the **ping** command. You can perform other operations only after Ping is finished or is interrupted by pressing **Ctrl+C**.

9.11 Traceroute

Before using Traceroute, you should configure the IP address and default gateway of the A10E/A28E.

Configure Traceroute for the A10E/A28E as below.

Step	Configuration	Description
1	Alpha-A28E# config	Enter global configuration mode.
2	Alpha-A28E(config)# interface ip <i>if-number</i>	Enter Layer 3 interface configuration mode.
3	Alpha-A28E(config-ip)# ip address <i>ip-address</i> [<i>ip-</i> <i>mask</i>] <i>vlan-id</i>	Configure the IP address of the interface.
4	Alpha-A28E(config-ip)# exit Alpha-A28E(config)# ip default-gateway <i>ip-address</i>	Configure the default gateway.
5	Alpha-A28E(config)# exit Alpha-A28E# traceroute <i>ip-</i> <i>address</i> [firstttl <i>first-</i> <i>ttl</i>] [maxttl <i>max-ttl</i>] [port <i>port-id</i>] [waittime <i>second</i>] [count <i>times</i>]	Test the connectivity of the IPv4 network, and show nodes passed by the packet.

10 Appendix

This chapter describes terms and abbreviations involved in this guide, including the following sections:

- Terms
- Abbreviations

10.1 Terms

A

Access
Control List
(ACL)

A series of orderable rules composed by permit | deny sentences. The device decides the packets to be received/refused based on these rules.

Automatic
Laser
Shutdown
(ALS)

A technology that is used for automatically turning the output power of laser and optical amplifier off to avoid personal injury.

Auto-
negotiation

The auto negotiation procedure is: the port at one site adapts its bit rate and duplex mode to the highest level that the opposite site device both support according to the bit rate and duplex mode adopted by the remote site device, that is, the connected devices on both site adopt the fastest transmission mode they both support after the auto negotiation process.

Automatic
Protection
Switching
(APS)

APS is used to monitor transport lines in real time and automatically analyze alarms to discover faults. When a critical fault occurs, APS can make the working channel switched to the protection channel quickly to recover communication in a very short period.

C

CFM

Connectivity Fault Management (CFM) is end to end service-level Ethernet OAM technology. This function is used to actively diagnose fault for Ethernet Virtual Connection (EVC) and provide cost-effective network maintenance solution via fault management function and improve network maintenance.

Challenge-Handshake Authentication Protocol (CHAP)	A protocol of PPP. It is a 3-times handshake authentication protocol which is used to transmit the user name only on the network.
D	
Dynamic ARP Inspection (DAI)	A security feature that can be used to verify the ARP datagram in the network. With DIA, the administrator can intercept, record, and discard ARP packets with invalid MAC address/IP address to prevent common ARP attacks.
Dynamic Host Configuration Protocol (DHCP)	A technology used for assigning IP address dynamically. It can automatically assign IP addresses for all clients in the network to reduce workload of the administrator. In addition, it can realize centralized management of IP addresses.
E	
Ear hanging	A component installed on both sides of the chassis, used for install the chassis to the rack.
Ethernet in the First Mile (EFM)	Complied with IEEE 802.3ah protocol, Ethernet in the First Mile (EFM) is a link-level Ethernet OAM technology. It provides the link connectivity detection function, link fault monitor function, and remote fault notification function, etc for a link between two directly connected devices. EFM is mainly used for Ethernet link on edges of the network accessed by users.
Ethernet Linear Protection Switching (ELPS)	An APS protocol based on ITU-T G.8031 Recommendation to protect an Ethernet link. It is an end-to-end protection technology, including two line protection modes: linear 1:1 protection switching and linear 1+1 protection switching.
Ethernet Ring Protection Switching (ERPS)	An APS protocol based on ITU-T G.8032 Recommendation to provide backup link protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer.
F	
Failover	Provide a port association solution, extending link backup range. Transport fault of upper layer device quickly to downstream device by monitoring upstream link and synchronize downstream link, then trigger switching between master and standby device and avoid traffic loss.
Full-duplex	Communication link can transmit and receive data at the same time from both directions.
G	

GFP encapsulation	Generic Framing Procedure (GFP) is a generic mapping technology. It can group variable-length or fixed-length data for unified adaption, making data service transmitted in multiple high-speed logistic transmission channels.
H	
Half-duplex	Refers to two-way electronic communication that takes place unidirectionally at a time. Communication between people is half-duplex when one person listens while the other speaks.
I	
Institute of Electrical and Electronics Engineers (IEEE)	An international Institute of electrical and Electronics Engineers. It is one of the largest technical organizations. It has more than 360,000 members in 175 countries (up to 2005).
Internet Assigned Numbers Authority (IANA)	It is mainly used to assign and maintain the unique code and value in Internet technology standard (protocol), such as the IP address or multicast address.
Internet Engineering Task Force (IETF)	It is established in 1985. It is the most authoritative technology and standard organization, which develops and formulate specifications related to the Internet.
L	
Label	A group of signals that are used to identify the cable, chassis, or warning.
Link aggregation	A computer networking term which describes using multiple network cables/ports in parallel to increase the link speed beyond the limits of any one single cable or port, and to increase the redundancy for higher availability.
Link Aggregation Control Protocol (LACP)	A protocol used for realizing link dynamic aggregation. LACP communicates with the peer by exchanging LACPDU.
M	
Multi-mode Fiber	Multi-mode can be transmitted in one fiber.
N	

Network Time Protocol (NTP)	A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed timer server and clients. NTP is used to perform clock synchronization on all devices in the network that support clock. Therefore, devices can provide different applications based on some time. In addition, NTP can ensure very high accuracy (about 10ms).
O	
Open Shortest Path First (OSPF)	An internal gateway dynamic routing protocol, which is used to decide the route in an Autonomous System (AS).
Optical Distribution Frame (ODF)	A distribution connection device between the fiber and a communication device. It is an important part of the optical transmission system. It is mainly used for fiber splicing, optical connector installation, fiber adjustment, additional pigtail storage, and fiber protection.
P	
Password Authentication Protocol (PAP)	A password authentication protocol of Point to Point Protocol. It is a twice handshake protocol used for transmitting the user name and password in a plain text.
Point-to-point Protocol over Ethernet (PPPoE)	With PPPoE, the remote device can control and account each access user.
Private VLAN (PVLAN)	PVLAN adopts Layer 2 isolation technology. Only the upper VLAN is visible globally. The lower VLANs are isolated from each other. If you partition each interface of the switch or IP DSLAM device into a lower VLAN, all interfaces are isolated from each other.
Protection ground wire	Cable to connect device to ground, usually it is co-axial cable in yellow and green
Q	
QinQ	QinQ is (also called Stacked VLAN or Double VLAN) extended from 802.1Q, defined by IEEE 802.1ad recommendation. Basic QinQ is a simple Layer 2 VPN tunnel technology, encapsulating outer VLAN Tag for client private packets at carrier access end, the packets take double VLAN Tag passing through trunk network (public network). In public network, packets only transmit according to outer VLAN Tag, the private VLAN Tag are transmitted as data in packets.

Quality of Service (QoS) A commonly-used performance indicator of a telecommunication system or channel. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio. It functions to measure the quality of the transmission system and the effectiveness of the services, as well as the capability of a service provider to meet the demands of users.

R

Rapid Spanning Tree Protocol (RSTP) RSTP is an extension of Spanning Tree Protocol, which realizes quick convergency of network topology.

Remote Authentication Dial In User Service (RADIUS) A protocol used to authenticate and account users in the network.

S

Simple Network Management Protocol (SNMP) A network management protocol defined by Internet Engineering Task Force (IETF) used to manage devices in the Internet. SNMP can make the network management system to remotely manage all network devices that support SNMP, including monitoring network status, modifying network device configurations, and receiving network event alarms. At present, SNMP is the most widely-used network management protocol in the TCP/IP network.

Simple Network Time Protocol (SNTP) SNTP is mainly used for synchronizing time of devices in the network.

Single-mode fiber Only a single mode can be transmitted in one fiber.

Spanning Tree Protocol (STP) STP can be used to eliminate network loops and back up link data. It blocks loops in logic to prevent broadcast storms. When the unblocked link fails, the blocked link is re-activated to act as the protection link.

V

Virtual Local Area Network (VLAN) VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segment logically rather than physically, thus implementing virtual work groups which are based on Layer 2 isolation and do not affect each other.

VLAN
Mapping

VLAN Mapping is mainly used to replace the private VLAN Tag of Ethernet packets with Carrier's VLAN Tag, making packets transmitted according to Carrier's VLAN forwarding rules. During packets are sent to the peer private network from the Carrier network, the VLAN Tag is restored to the original private VLAN Tag, according to the same VLAN forwarding rules. Therefore packets are correctly sent to the destination.

10.2 Abbreviations

A	
AAA	Authentication, Authorization and Accounting
ABR	Area Border Router
AC	Alternating Current
ACL	Access Control List
ANSI	American National Standards Institute
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
AS	Autonomous System
ASCII	American Standard Code for Information Interchange
ASE	Autonomous System External
ATM	Asynchronous Transfer Mode
AWG	American Wire Gauge
B	
BC	Boundary Clock
BDR	Backup Designated Router
BITS	Building Integrated Timing Supply System
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BTS	Base Transceiver Station
C	
CAR	Committed Access Rate
CAS	Channel Associated Signaling

CBS	Committed Burst Size
CE	Customer Edge
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CST	Common Spanning Tree
D	
DAI	Dynamic ARP Inspection
DBA	Dynamic Bandwidth Allocation
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Service
DNS	Domain Name System
DRR	Deficit Round Robin
DS	Differentiated Services
DSL	Digital Subscriber Line
E	
EAP	Extensible Authentication Protocol
EAPoL	EAP over LAN
EFM	Ethernet in the First Mile
EMC	Electro Magnetic Compatibility
EMI	Electro Magnetic Interference
EMS	Electro Magnetic Susceptibility
ERPS	Ethernet Ring Protection Switching
ESD	Electro Static Discharge

EVC	Ethernet Virtual Connection
F	
FCS	Frame Check Sequence
FE	Fast Ethernet
FIFO	First Input First Output
FTP	File Transfer Protocol
G	
GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GMRP	GARP Multicast Registration Protocol
GPS	Global Positioning System
GVRP	Generic VLAN Registration Protocol
H	
HDLC	High-level Data Link Control
HTTP	Hyper Text Transfer Protocol
I	
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IE	Internet Explorer
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System Routing Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector

L

LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LAN	Local Area Network
LCAS	Link Capacity Adjustment Scheme
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit

M

MAC	Medium Access Control
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface cross-over
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Between Failure
MTU	Maximum Transmission Unit
MVR	Multicast VLAN Registration

N

NMS	Network Management System
NNM	Network Node Management
NOS	Network Operating System
NTP	Network Time Protocol
NView NNM	NView Network Node Management

O

OAM	Operation,Administration and Management
OC	Ordinary Clock
ODF	Optical Distribution Frame
OID	Object Identifiers
Option 82	DHCP Relay Agent Information Option
OSPF	Open Shortest Path First

P	
P2MP	Point to Multipoint
P2P	Point-to-Point
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADS	PPPoE Active Discovery Session-confirmation
PAP	Password Authentication Protocol
PDU	Protocol Data Unit
PE	Provider Edge
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
Ping	Packet Internet Grope
PPP	Point to Point Protocol
PPPoE	PPP over Ethernet
PTP	Precision Time Protocol
Q	
QoS	Quality of Service
R	
RADIUS	Remote Authentication Dial In User Service
RED	Random Early Detection
RH	Relative Humidity
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
RPL	Ring Protection Link
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource Reservation Protocol
S	
SCADA	Supervisory Control And Data Acquisition
SF	Signal Fail

SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SPF	Shortest Path First
SSHv2	Secure Shell v2
STP	Spanning Tree Protocol
T	
TACACS+	Terminal Access Controller Access Control System
TC	Transparent Clock
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
U	
UDP	User Datagram Protocol
UNI	User Network Interface
USM	User-Based Security Model
V	
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
W	
WAN	Wide Area Network
WRR	Weight Round Robin

